Federal Office
for Information Security

Deutschland
Digital•Sicher•BSI•

# Securing the Supply Chain Together – Through Automation of Advisories and Vulnerability Management

Jens Wiesner & Thomas Schmidt
Federal Office for Information Security (BSI)

# Who are we?

**Jens Wiesner**

Team Lead ICS @BSI
(traveling presenter,
Saying important things to important people)

Responsible for Critical Infrastructure Protection

- Publishing Best Practices
- Assessing impact of vulnerabilities in CI
- Making the world a better place

**Thomas Schmidt**

Technical ICS Analyst @BSI
(usually not into standardization)

First day at work: analyze TRITON / TRISIS
Passion for

- ICS
- International Cooperation
- CVD
- Capacity building

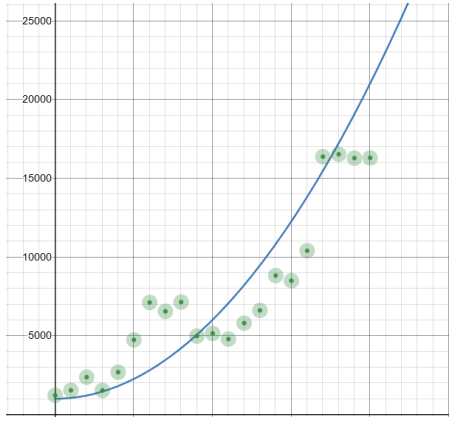
# Difference between Vulnerabilities and Advisories

**Vulnerability (CVE)**

- Can be discovered by anybody
  - Security researcher (hacker)
  - Vendor
  - User
- Usually for one product
  (although much more may be affected)
- Coordinated Vulnerability Disclosure Program should be established by the vendor,
  (BSI Publication on Vulnerability Handling)
- Huge amount published each year in NVD
  > 28000 in 2021
- Use RFC 9116 (security.txt)

**Advisory**

- Usually supplied by the vendor / maintainer of the software
- May cover multiple CVE
- Describes Patch and/or Mitigating countermeasures
- Takes some time to publish
- Often part of a support agreement




https://opensourcesecurity.io/2021/03/30/its-time-to-fix-cve/

# Target audience should be interested in advisories

| How to | Producer of | | Consumer of | |
|---|---|---|---|---|
| | Vulnerability Reports | Advisories | Vulnerability Reports | Advisories |
| Write | o | ++ | - | - |
| Generate | o | ++ | - | - |
| Automate | o | ++ | o | o |
| Upload / Publish | o | ++ | - | - |
| Find / retrieve | - | - | o | ++ |
| Modify / Enrich | o | ++ | - | - |

# Agenda

1. Presenting CSAF
2. 1st exercise analysis of a CSAF Document + writing own advisories (Secvisogram)
3. Break & Solving Technical Issues
4. 2nd exercise Publish
5. 3rd exercise Retrieve CSAF Documents
6. 4th exercise Update existing CSAF Documents
7. 5th exercise CSAF Aggregator
8. Bonus exercise A: Push CSAF to ticket system or CSAF management system
9. Bonus exercise B: Compare a CSAF document with an SBOM or asset database
10. Bonus exercise C: Modify other CSAF Document

# Key takeaways

- Securing the supply chain is necessary
- You can't secure the supply chain on your own - it works only together
- Automation is possible and reduces human workload
- CSAF is a step towards a more secure supply chain through automation

# Workshop instructions

# Basics

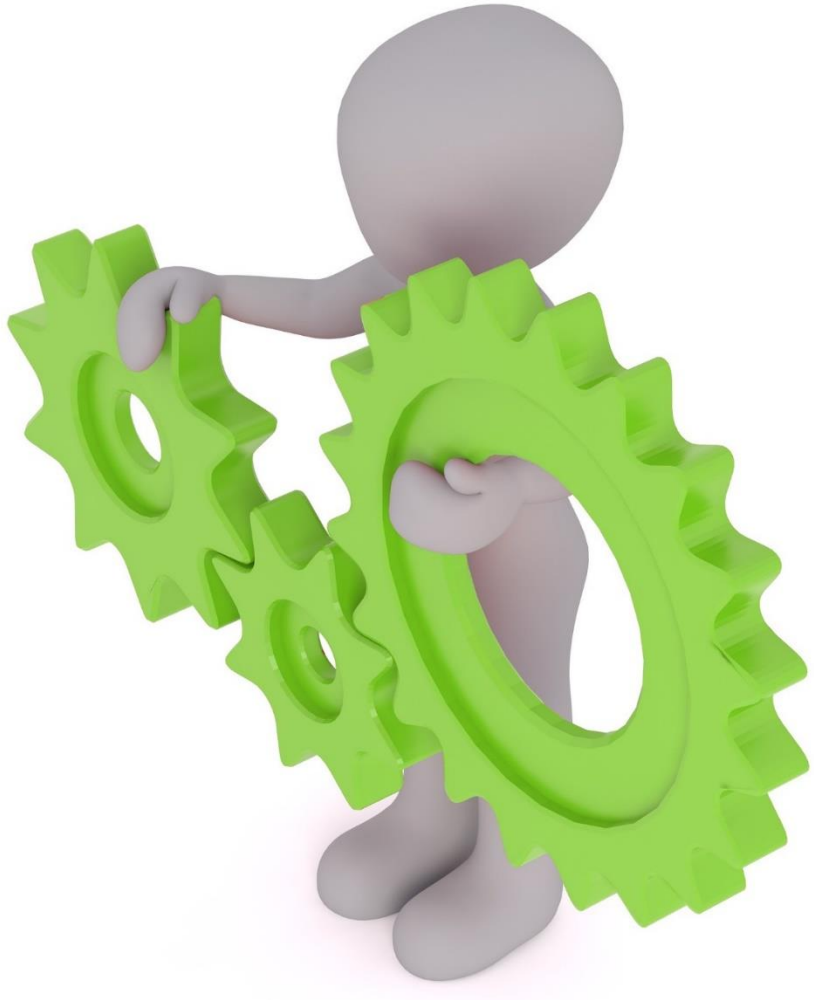
# Why are Advisories important?

- Knowing the existence of a vulnerability is not enough
- Actions must be taken:
  - Assessing the risk
  - Assessing the cost

→ Relevant information is in the security advisory

# Why is Vulnerability Management important?

- Prioritization:
  - Which vulnerability is patched first / most important?
  - How do I distribute my resources?
- Tracking:
  - Who is doing what?
  - How long does our process take?
  - What risk do I have?
- Scaling:
  - Multiple sources of information
  - Multiple vendors
  - Don’t forget anything.



But why do we need to automate things?

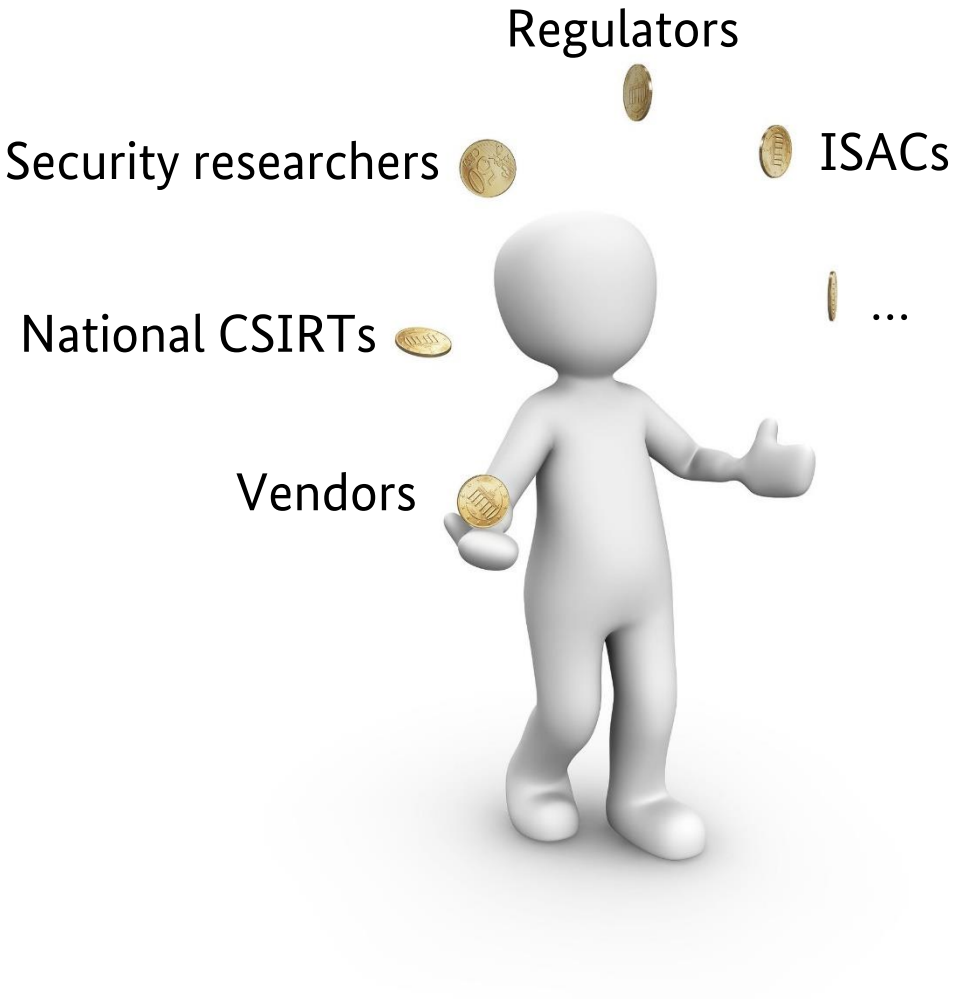
# Asset Owners want to run their facility

Machines
Factory lines
Whole installations
Usually comprise of several different vendors

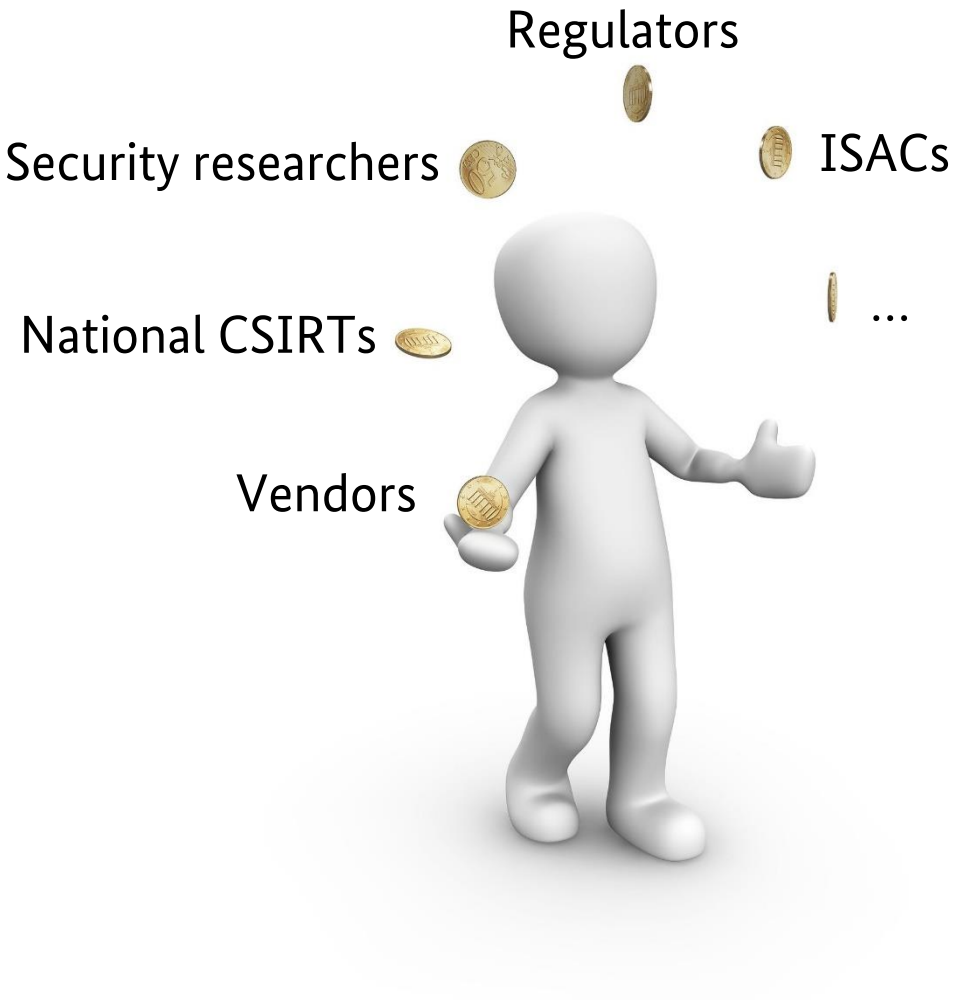
# Asset Owners are confronted with a lot of things


Federal Office for Information Security

# So many sources of information – some examples



# So many sources of information – so many channels and formats







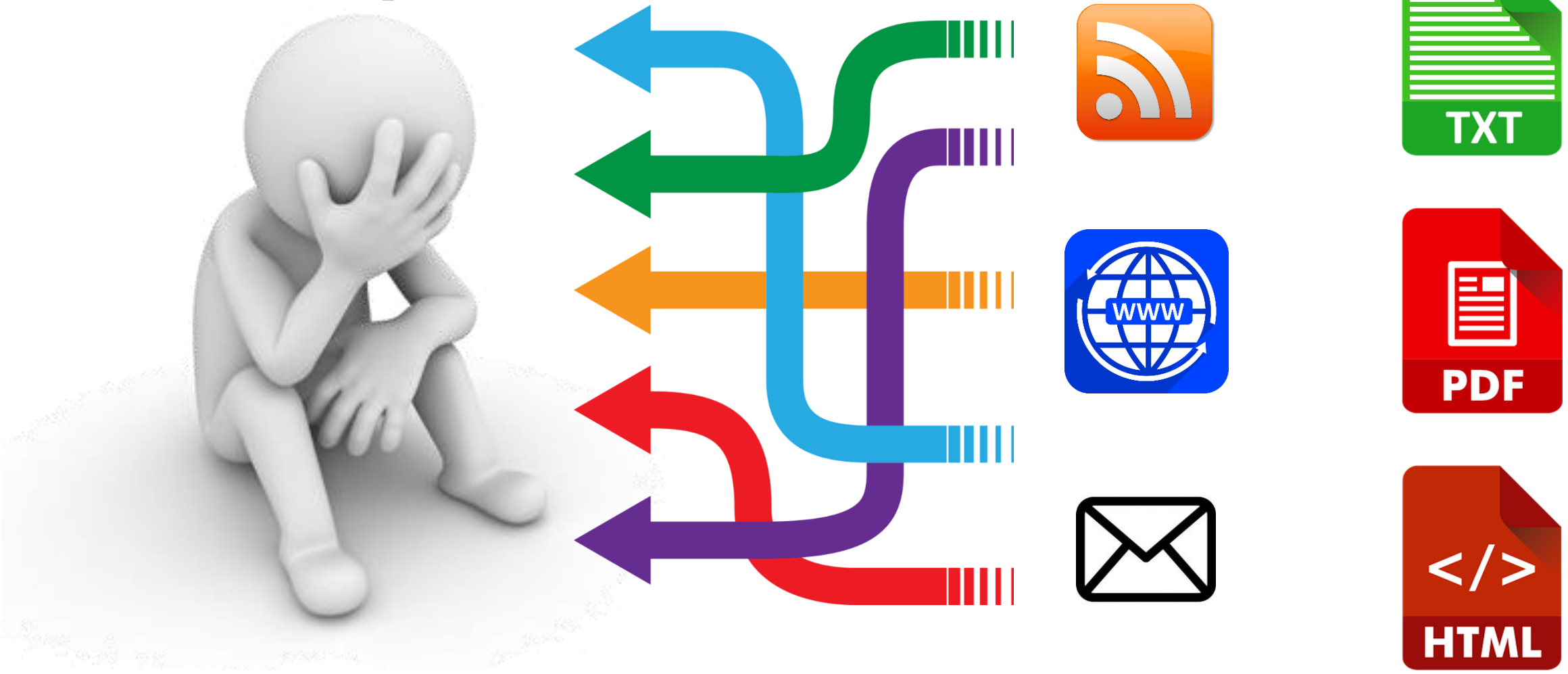






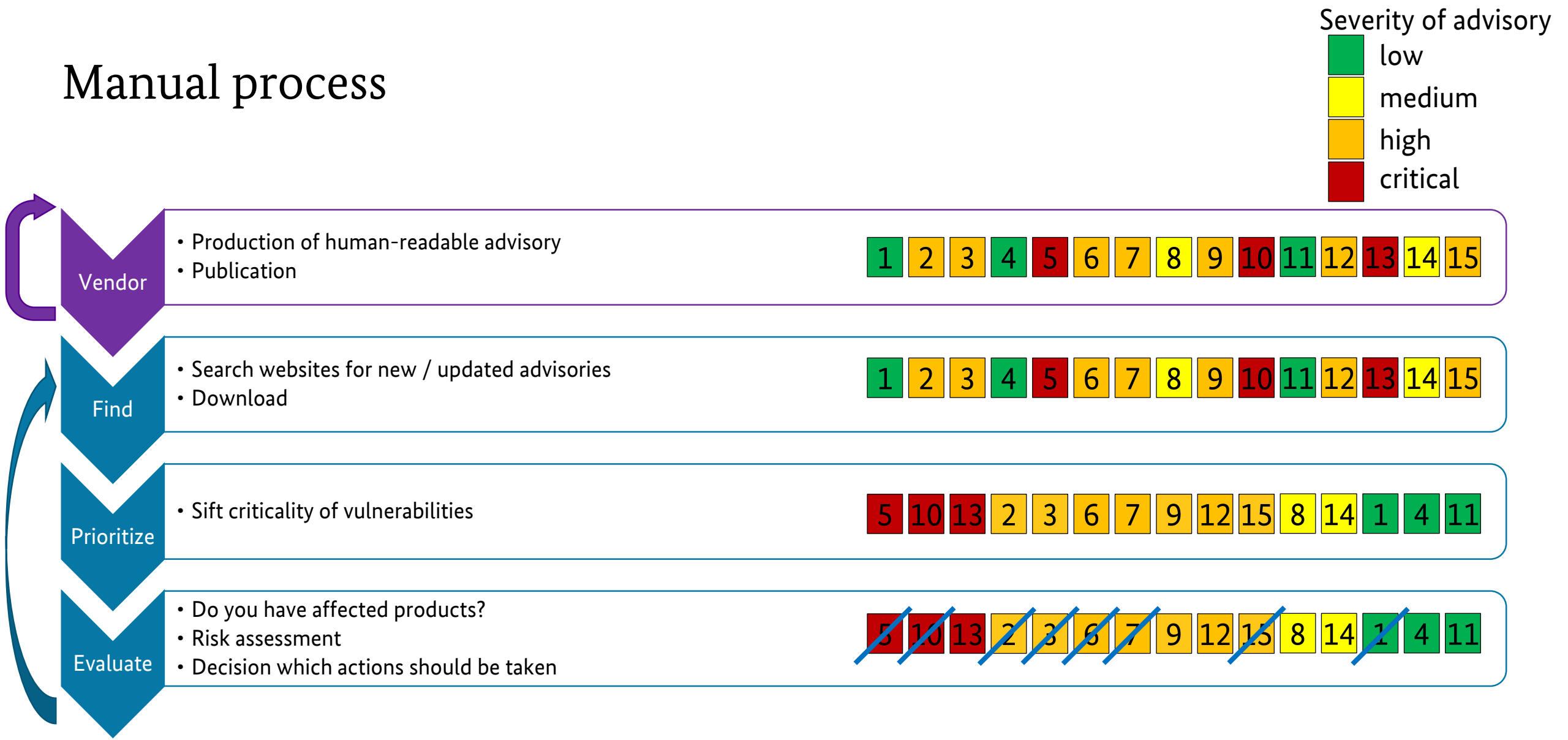

Federal Office for Information Security

# What should an operator / asset owner do?
# Patches and updates!



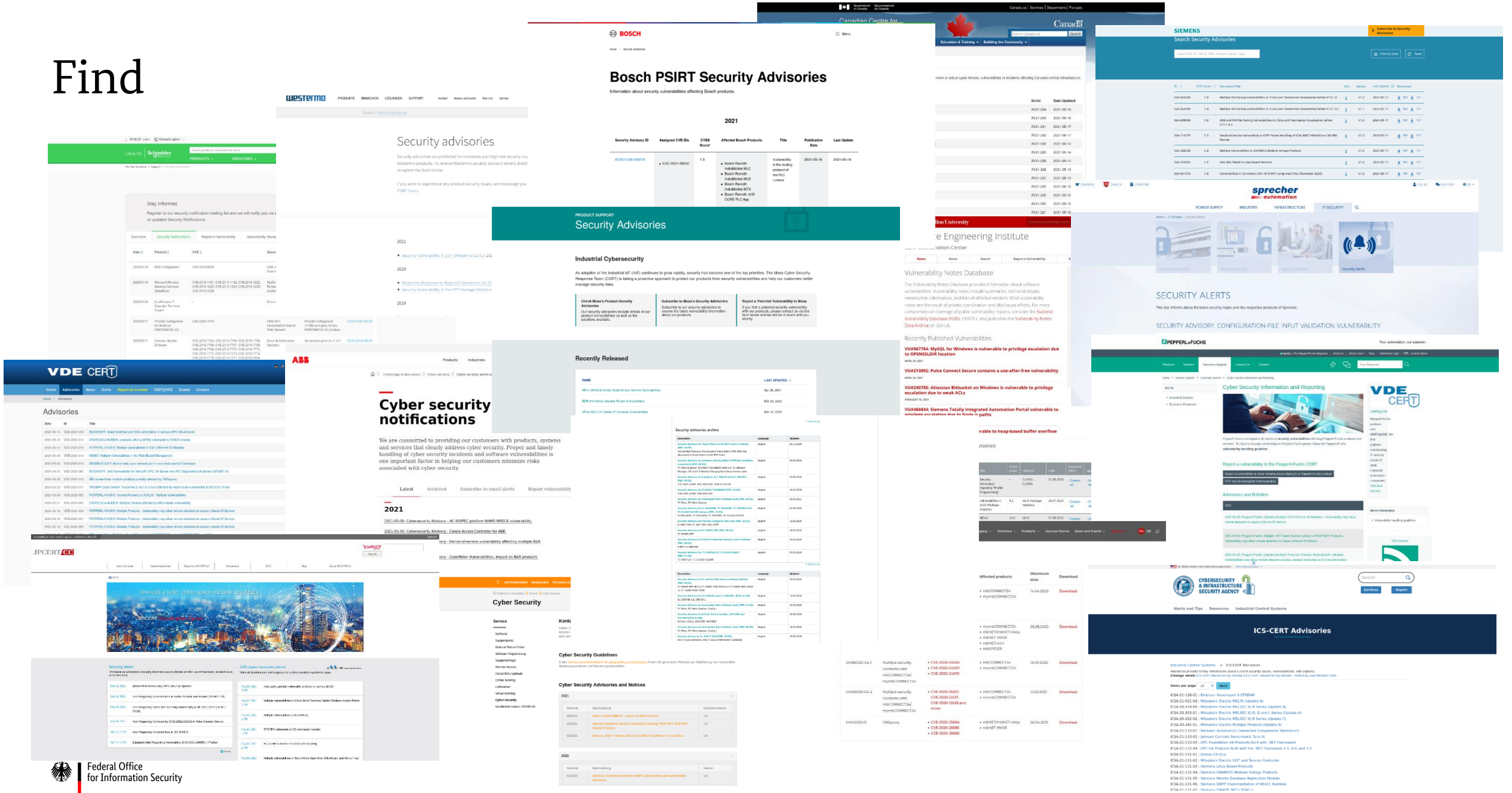

Federal Office
for Information Security

# Manual process




Federal Office for Information Security

# Find


BOSCH
Bosch PSIRT Security Advisories
Information about security vulnerabilities affecting Bosch products.
2021
Security Advisory ID
Assigned CVE IDs
CVSS Score
Affected Bosch Products
Title
Publication Date
Last Update
Canada
Canadian Centre for
SIEMENS
Search Security Advisories
westermo
PRODUKTE
BRANCHEN
LÖSUNGEN
SUPPORT
Security advisories
Stay Informed
PRODUCT SUPPORT
Security Advisories
Industrial Cybersecurity
Recently Released
sprecher automation
SECURITY ALERTS
SECURITY ADVISORY, CONFIGURATION-FILE INPUT VALIDATION VULNERABILITY
VDE CERT
Advisories
ABB
Cyber security notifications
We are committed to providing our customers with products, systems and services that clearly address cyber security. Proper and timely handling of cyber security incidents and software vulnerabilities is one important factor in helping our customers minimize risks associated with cyber security.
Latest
Archived
Subscribe to email alerts
Report vulnerability
2021
2021-05-06: Cybersecurity Advisory - AC 800PEC platform NAME:WRECK vulnerability
2021-05-06: Cybersecurity Advisory - Cassia Access Controller for ABB
Cyber Security
Cyber Security Guidelines
Cyber Security Advisories and Notices
Vulnerability Notes Database
Recently Published Vulnerabilities
VU#587764: MySQL for Windows is vulnerable to privilege escalation due to OPENSSLDIR location
VU#213092: Pulse Connect Secure contains a use-after-free vulnerability
VU#240785: Atlassian Bitbucket on Windows is vulnerable to privilege escalation due to weak ACLs
VU#446044: Siemens Totally Integrated Automation Portal vulnerable to
PEPPERL+FUCHS
Cyber Security Information and Reporting
Advisories and Bulletins
JPCERT CC
Towards a safer cyber space without incidents
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
ICS-CERT Advisories

# Analyze

An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Search

Services Report

Alerts and Tips Resources Industrial Control Systems

Industrial Control Systems > ICS-CERT Advisories > Emerson Rosemount X-STREAM

## ICS Advisory (ICSA-21-138-01)

More ICS-CERT Advisories

### Emerson Rosemount X-STREAM

Original release date: May 18, 2021

Print Tweet Send Share


### Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is ... ent of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commerci ... or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see h...

### 1. EXECUTIVE SUMMARY

- CVSS v3 7.5
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Emerson
- **Equipment:** Rosemount X-STREAM Gas Analyzer
- **Vulnerabilities:** Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Type, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Improper Restriction of Rendered UI Layers or Frames

### 2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to obtain sensitive information, modify configuration, or affect the availability of the device.

### 3. TECHNICAL DETAILS

#### 3.1 AFFECTED PRODUCTS

Life Is On Schneider Electric

## Schneider Electric Security Notification

### EcoStruxure Geo SCADA Expert

11 May 2021

#### Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure Geo SCADA Expert products (formerly known as ClearSCADA).

The EcoStruxure Geo SCADA Expert product is an open, flexible and scalable software system for telemetry and remote SCADA solutions.

Failure to apply the remediations provided below may risk the revealing of account credentials, which could result in unauthorized system access.

#### Affected Products and V...

- ClearSCADA, all ver...
- EcoStruxure Geo SC...
- EcoStruxure Geo SC...


#### Vulnerability Details

CVE ID: CVE-2021-22741

CVSS v3.1 Base Score 6.7 ...:N/S:U/C:H/I:H/A:H

A *CWE-916: Use of Passwo... Effort* vulnerability exists that could cause the r... ver database files are available. Exposure of these ... n vulnerable to password decryption attacks. Note tha... contain user account password hashes.

#### Remediation

Geo SCADA Expert 2020 April 2021 (83.7787.1) includes a fix for this vulnerability. The security of stored passwords in the servers is significantly strengthened. It is available for download here:

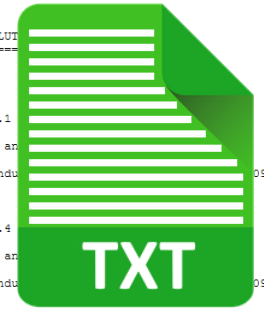
https://tprojects.schneider-electric.com/telemetry/display/CS/Geo+SCADA+Expert+Downloads

Installation of new server software will require system restart or changeover of redundant servers. Consult the Release Notes and Resource Center for advice on the procedure.

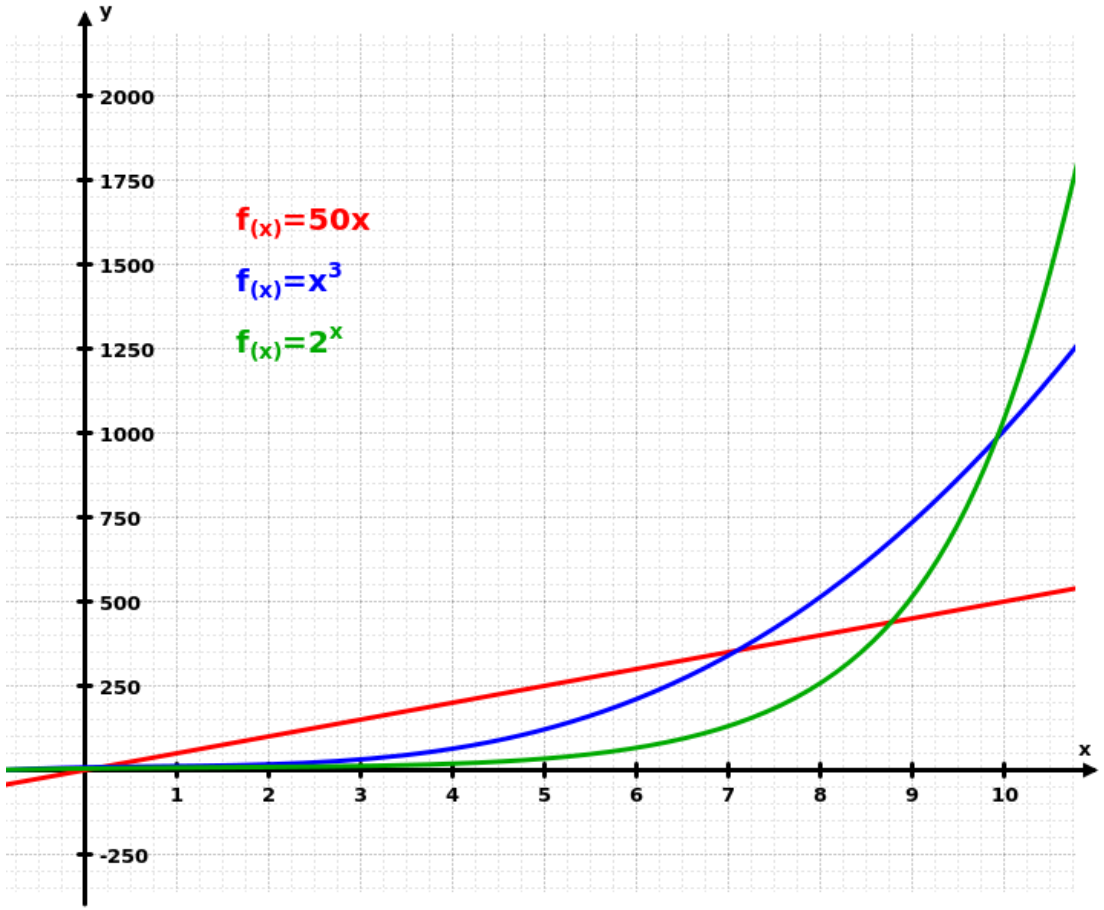
Customers should use appropriate update methodologies when applying these updates to their systems. We strongly recommend the use of back-ups and evaluating the impact of these updates in a Test and Development environment or on an offline infrastructure.



```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

# SSA-344983: Vulnerability in WPA2 Key Handling affecting SCALANCE W700 and SCALANCE
W1700 Devices

Publication Date:        2019-12-10
Last Update:             2019-12-10
Current Version:         1.0
CVSS v3.1 Base Score:    6.5

SUMMARY
=======

The latest firmware updates for the SCALANCE W700 and W1700 wireless
device families fix a vulnerability affecting WPA/WPA2 key handling. It
might be possible to, by manipulating the EAPOL-Key frames, decrypt the
Key Data field without the frame being authenticated.

This has impact on WPA/WPA2 architectures using TKIP encryption. The
attacker must be in the wireless range of the device to perform the
attack.

AFFECTED PRODUCTS AND SOLUT...
==========================


* SCALANCE W1700
  - Affected versions:
       All versions < V1.1
  - Remediation:
       Update to V1.1 or an...
  - Download:
       https://support.indu...09762253

* SCALANCE W700
  - Affected versions:
       All versions < V6.4
  - Remediation:
       Update to V6.4 or an...
  - Download:
       https://support.indu...09773308

WORKAROUNDS AND MITIGATIONS
===========================

Siemens has identified the following specific workarounds and mitigations that
customers can apply to reduce the risk:

* Whenever possible, use AES-CCMP instead of TKIP in the WPA/WPA2
networks. This can be configured for both SCALANCE W-700 and W-1700
families over the Web Based Management (web server). For more
information, go for the respective Manual.


GENERAL SECURITY RECOMMENDATIONS
================================

As a general security measure, Siemens strongly recommends to protect
network access to devices with appropriate mechanisms. In order to
operate the devices in a protected IT environment, Siemens recommends to
configure the environment according to Siemens' operational guidelines
for Industrial Security (Download:
https://www.siemens.com/cert/operational-guidelines-industrial-security),
and to follow the recommendations in the product manuals.
```

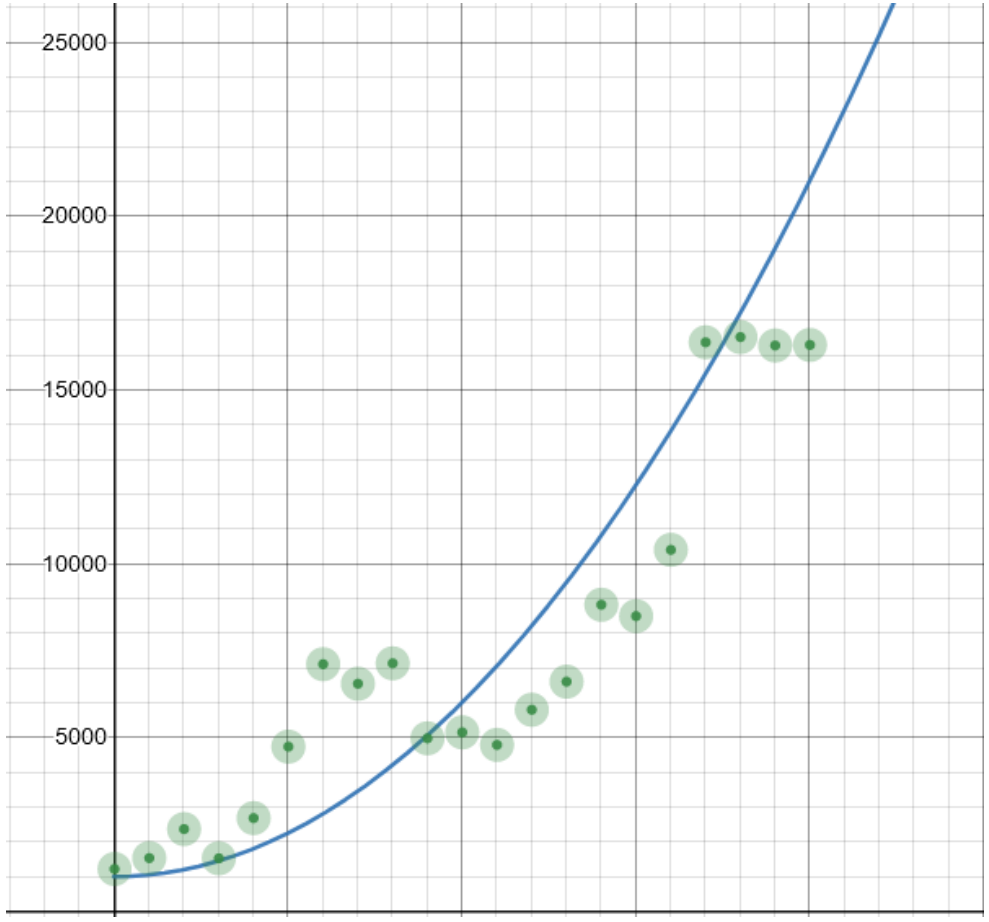


# Number of Advisories




https://upload.wikimedia.org/wikipedia/commons/6/64/Exponential.svg

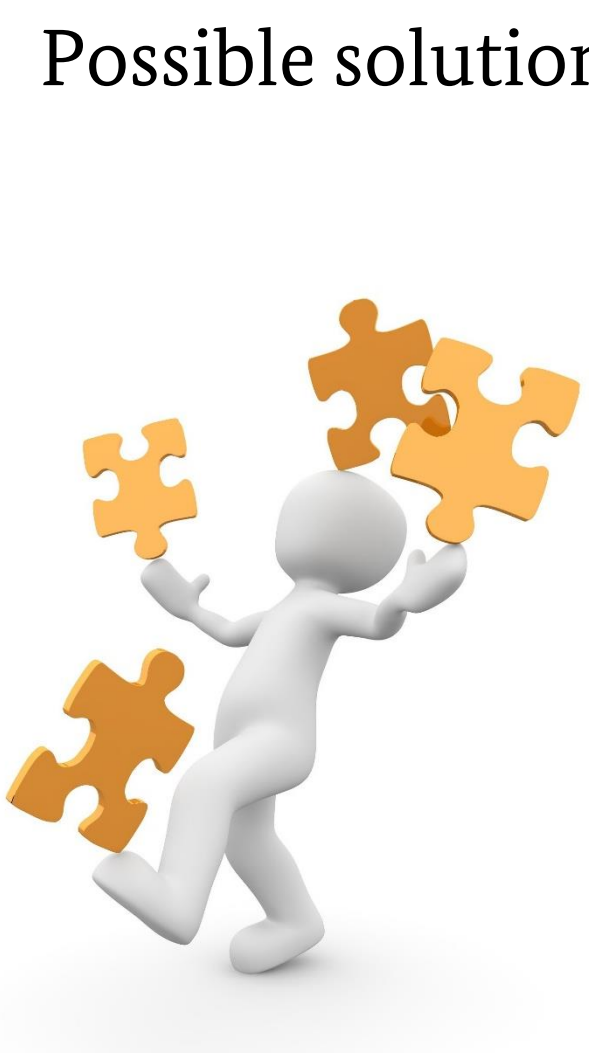
# Number of ~~Advisories~~ CVE

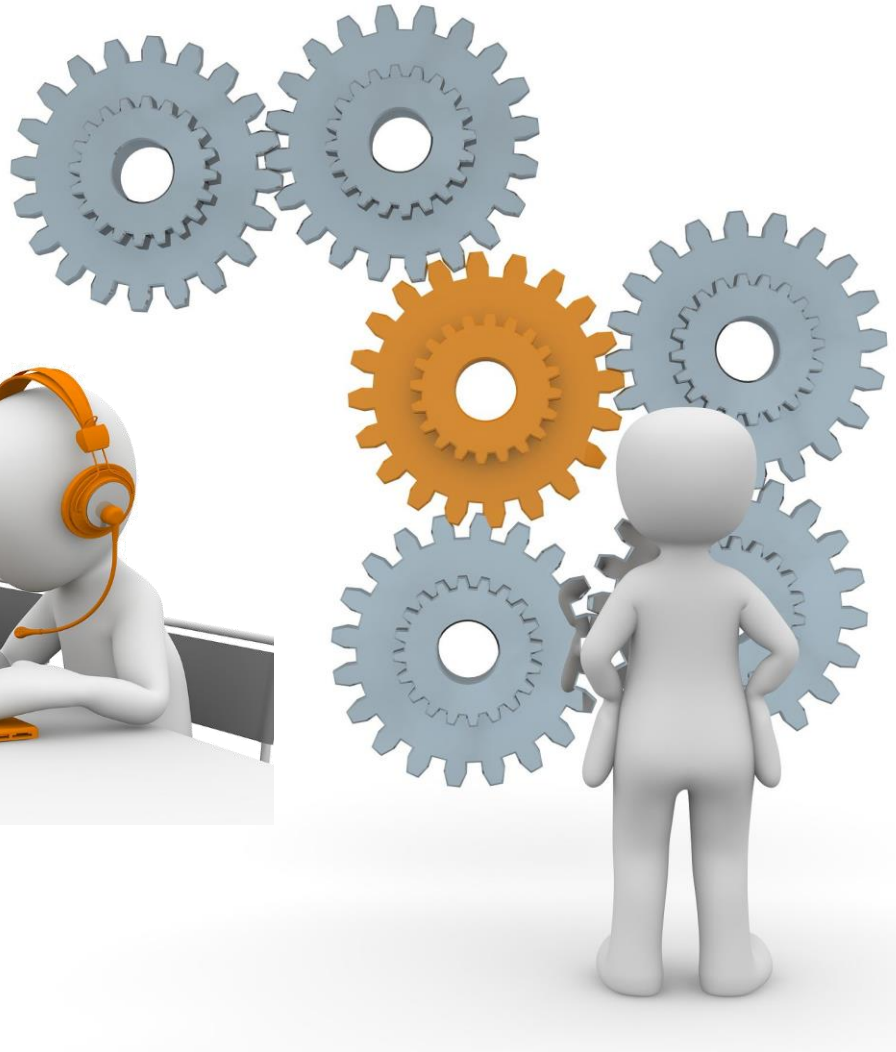



https://opensourcesecurity.io/2021/03/30/its-time-to-fix-cve/

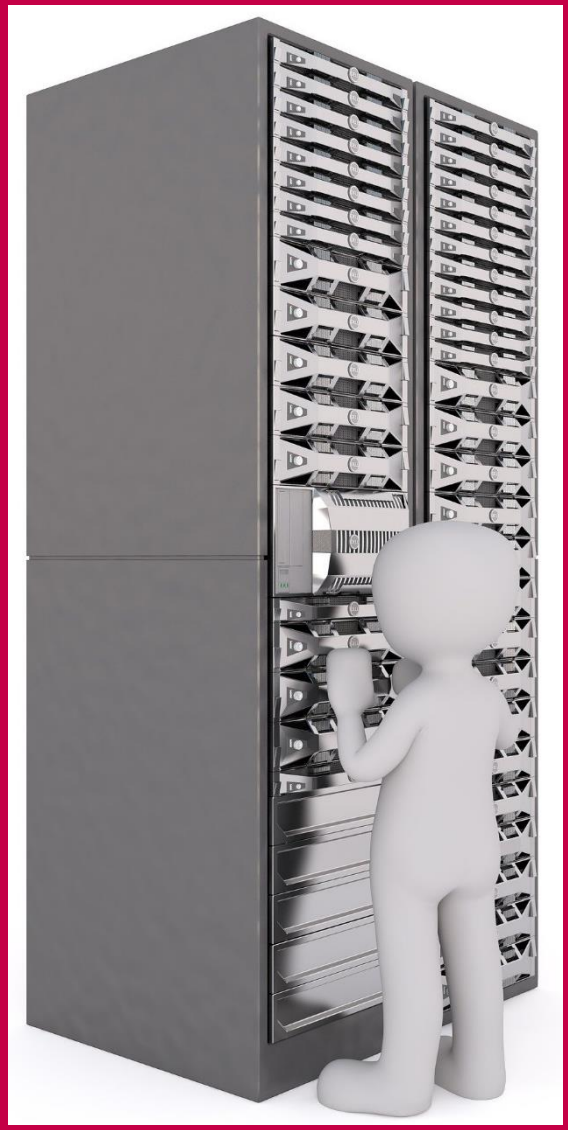
That doesn‘t scale!

# Possible solutions

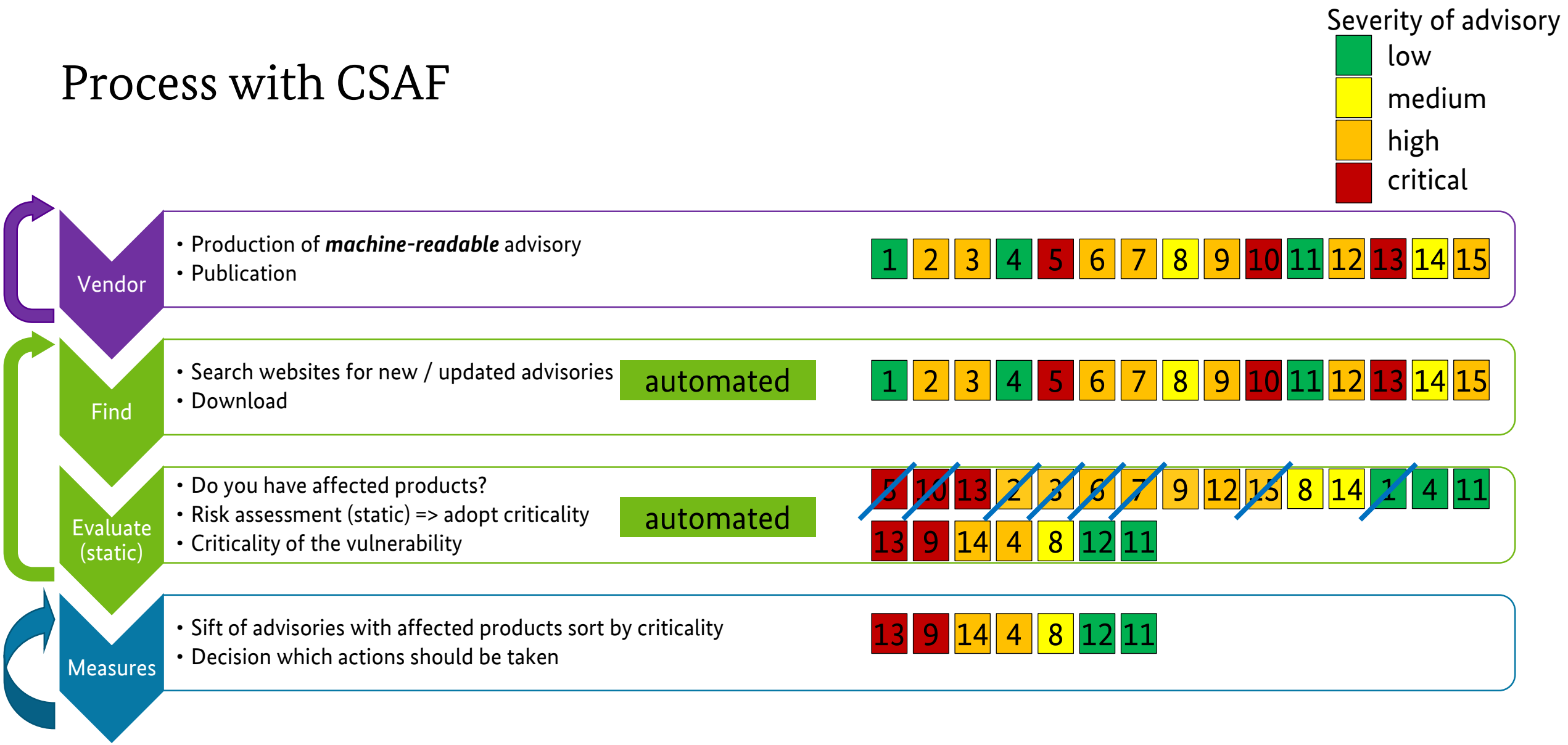




Let’s automate the process…



# Process with CSAF




Federal Office for Information Security

# What is CSAF?

**Common Security Advisory Framework**

- Machine-readable format for security advisories (JSON)
- Standardized way of distribution security advisories
- Build with automation in mind
- Standardized tool set
- Guidance to actionable information
- Successor of CSAF CVRF 1.2


Ready to use!

# Who is involved in the development of CSAF?

- AT&T
- Cisco
- Microsoft
- Red Hat
- Oracle
- Siemens
- BSI
- ...

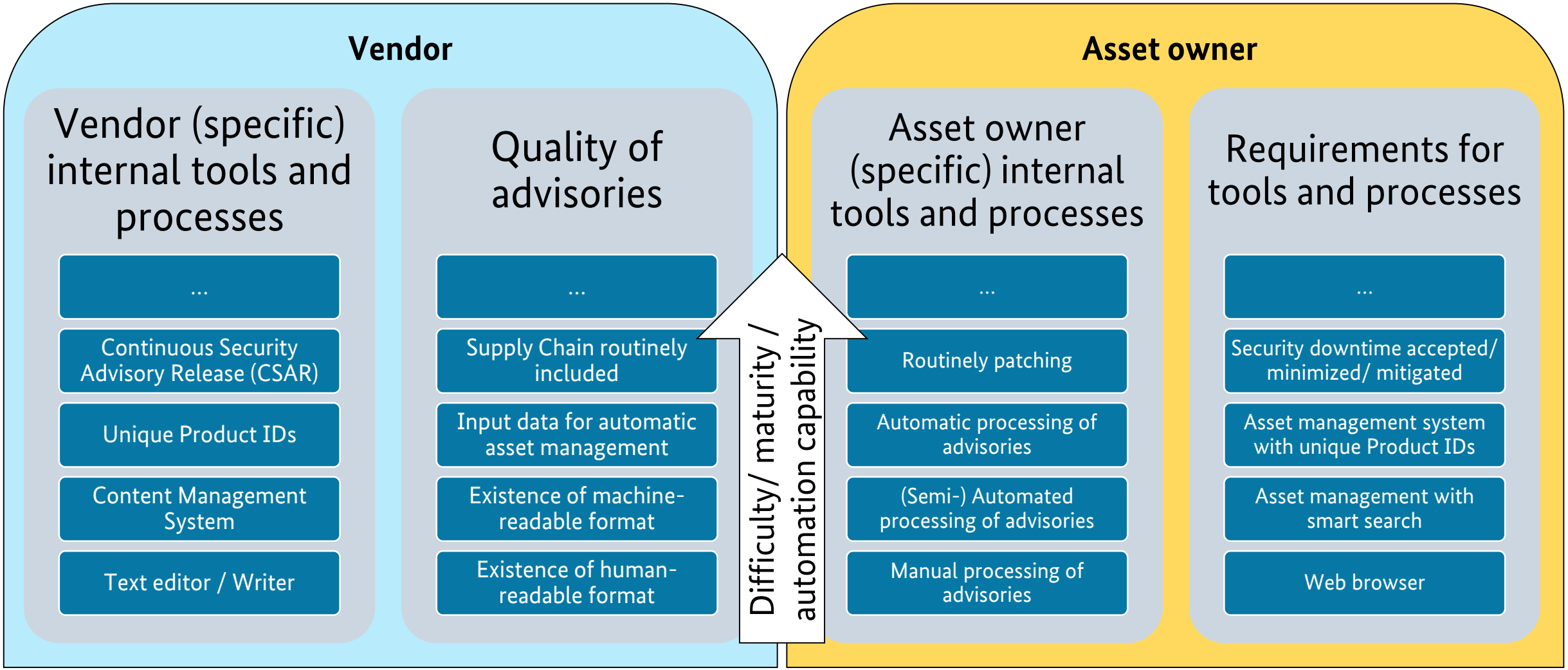
See full list at: https://www.oasis-open.org/committees/membership.php?wg_abbrev=csaf

We need your support to make it work!

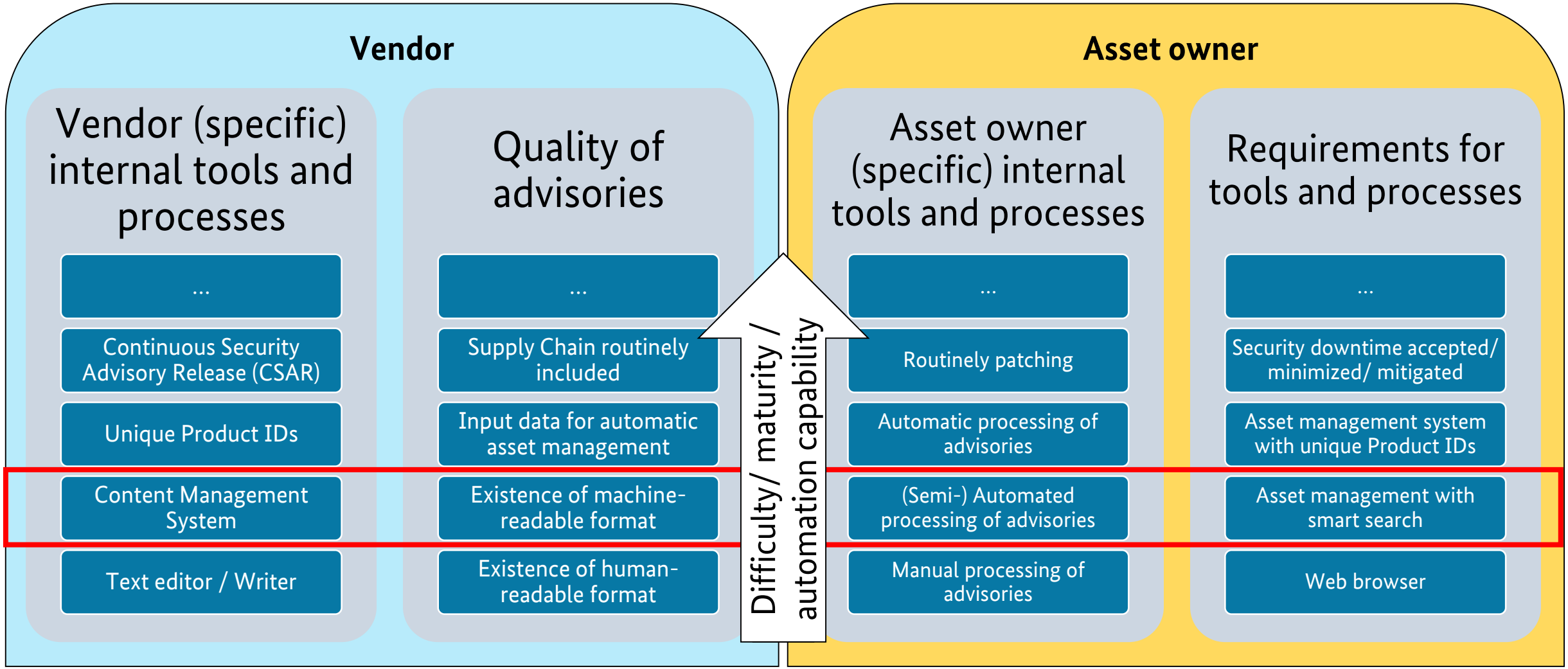
# Benefits for asset owners

- Makes the impossible (stringent patch and update management) **possible** (at the moment often sporadic or dependent on personal availability/interests)
- **Reduce** human factor and individual work load
  - No more manual searching for advisories
  - Easier to determine affected devices
  - Delegable
  - See only relevant advisories
- **Scalable** across all participating vendors
- Enables basic risk assessment based on own environment

# Two sides of the same coin – different maturity stages



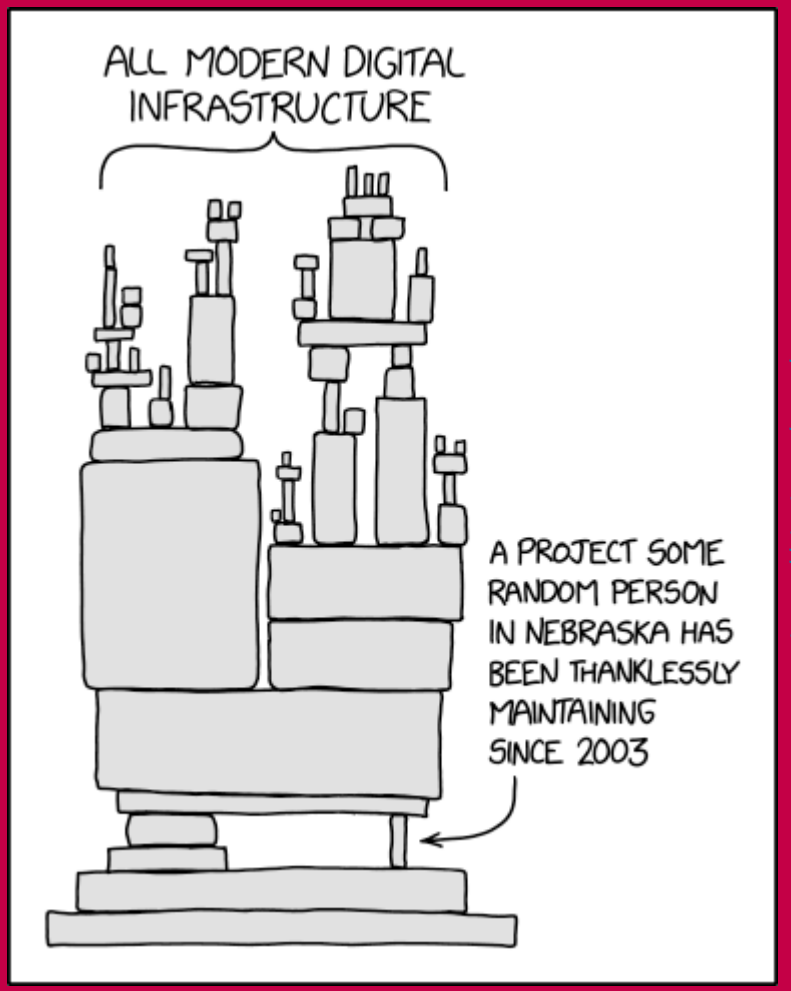
# Next step: reach stage 2 across parties



# Requirements for asset owners

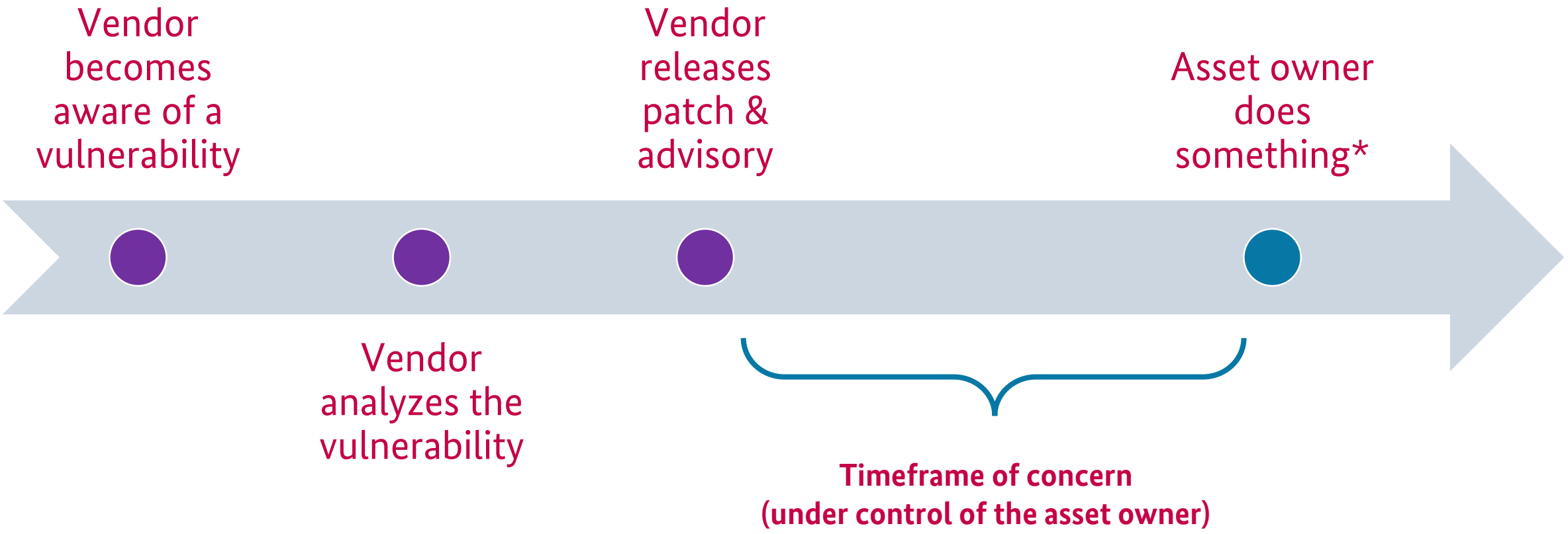
- Machine-readable asset inventory
- Request Advisories in CSAF from vendors
- Connection between both of them to leverage the full potential

How does that help in the supply chain?




https://xkcd.com/2347/

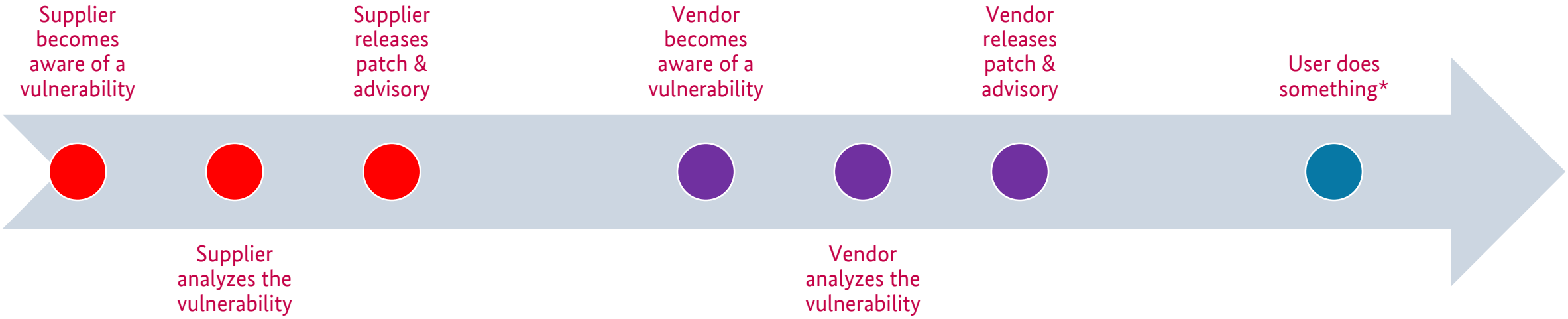
# Timeframe of concern




Federal Office for Information Security

* Patch, mitigate risk, or actively accept risk

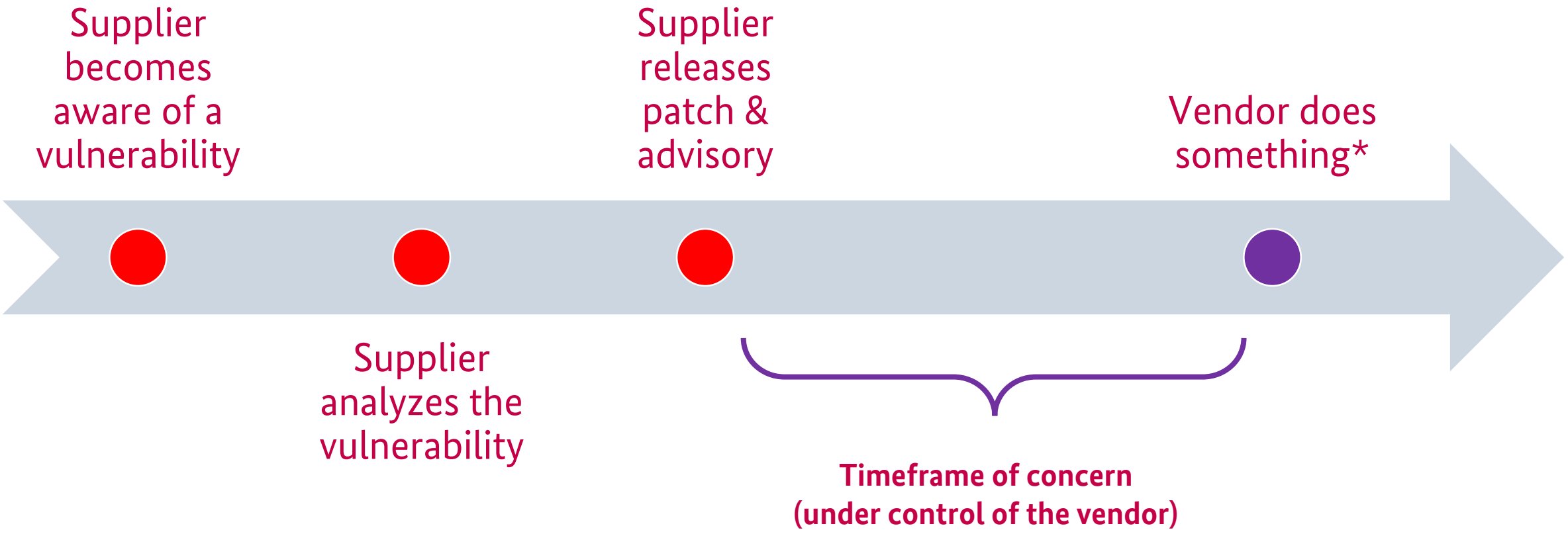
# Supply chain




Federal Office for Information Security

* Patch, mitigate risk, or actively accept risk

# (Almost) Every vendor is a user




Federal Office for Information Security

* Patch, mitigate risk, or actively accept risk

# PART II

# Where to find basic information?
# https://csaf.io

| | |
|---|---|
| OASIS TC: CSAF website: | https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf |
| CSAF GitHub: | https://github.com/oasis-tcs/csaf |
| CSAF 2.0 JSON Schema: | https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/json_schema/csaf_json_schema.json |
| **CSAF 2.0 Prose:** | https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/prose/csaf-v2-editor-draft.md |
| **CSAF 2.0 Examples:** | https://github.com/oasis-tcs/csaf/tree/master/csaf_2.0/examples |
| Secvisogram sources: | https://github.com/secvisogram/secvisogram |
| **Running Demo:** | **https://secvisogram.github.io** |

# Exercise 1

Write an advisory in CSAF

# Example CSAF Document




```
{
  "document": {
    "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
    "category": "Cisco Security Advisory",
    "csaf_version": "2.0",
    "publisher": {
    "tracking": {
      "id": "cisco-sa-20180328-smi2",
      "status": "final",
      "version": "3.0.0",
      "revision history": [
      "initial_release_date": "2018-03-28T16:00:00Z",
      "current_release_date": "2018-04-17T15:08:41Z",
      "generator": {
    },
    "notes": [
    "references": [
      {
        "url": "https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2",
        "summary": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability"
      }
    ]
  },
  "product_tree": {
    "branches": [
  },
  "vulnerabilities": [
    {
      "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
      "ids": [
      "notes": [
      "cve": "CVE-2018-0171",
      "product_status": {
        "known_affected": [
      },
      "scores": [
      "remediations": [
      ],
      "references": [
    }
  ]
}
```

# Example CSAF Document

Document level metadata

Product tree

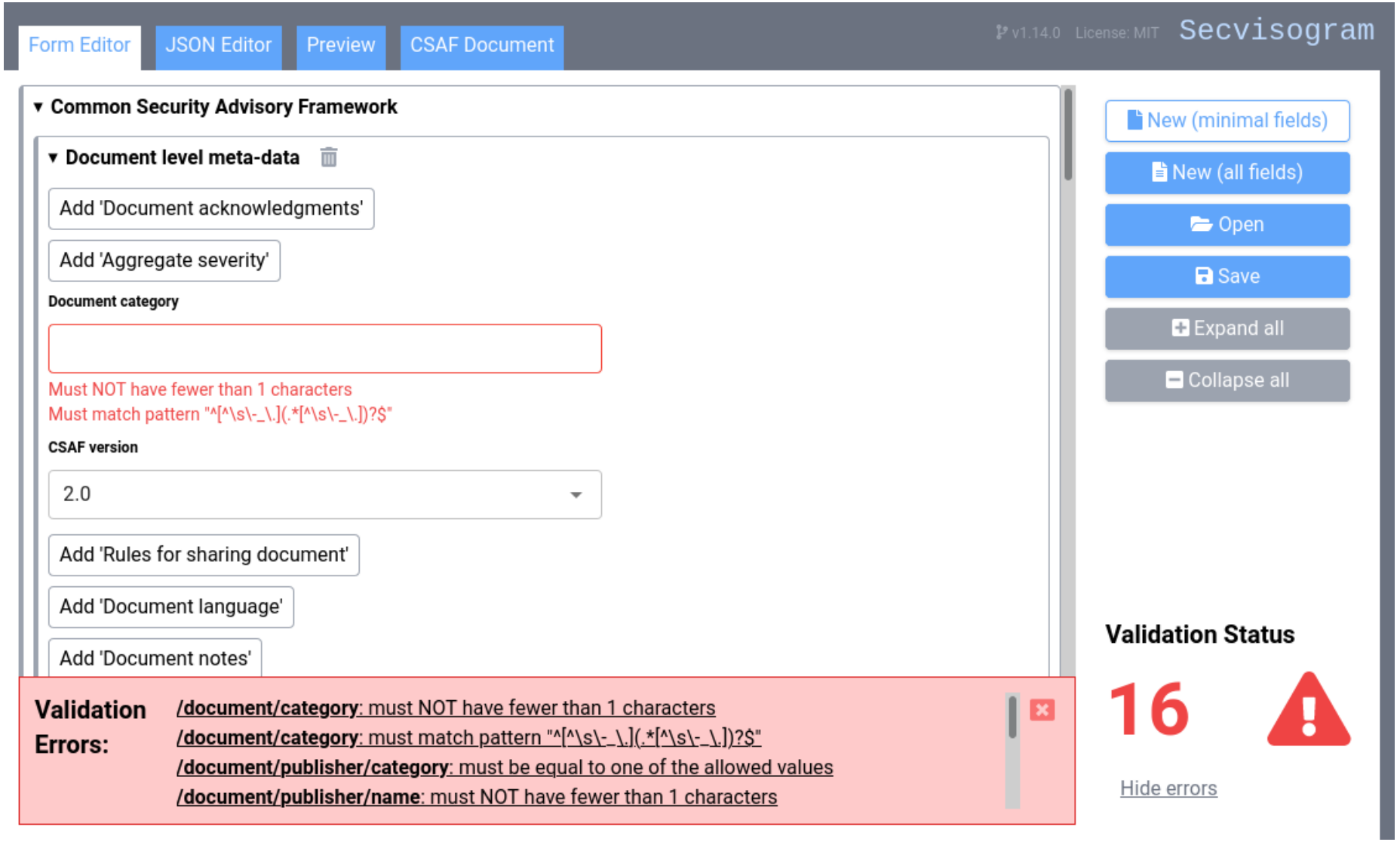
Vulnerabilities




```
{
  "document": {
    "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
    "category": "Cisco Security Advisory",
    "csaf_version": "2.0",
    "publisher": {
    "tracking": {
      "id": "cisco-sa-20180328-smi2",
      "status": "final",
      "version": "3.0.0",
      "revision history": [
      "initial_release_date": "2018-03-28T16:00:00Z",
      "current_release_date": "2018-04-17T15:08:41Z",
      "generator": {
    },
    "notes": [
    "references": [
      {
        "url": "https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2",
        "summary": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability"
      }
    ]
  },
  "product_tree": {
    "branches": [
  },
  "vulnerabilities": [
    {
      "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
      "ids": [
      "notes": [
      "cve": "CVE-2018-0171",
      "product_status": {
        "known_affected": [
      },
      "scores": [
      "remediations": [
      ],
      "references": [
    }
  ]
}
```

# Secvisogram

https://secvisogram.github.io



# Break

# One problem solved: unified format specified

# Exercise 2

Publish a CSAF document

# Excurse RFC 9116 / security.txt

"When security risks in web services are discovered by independent security researchers who understand the severity of the risk, they often lack the channels to disclose them properly. As a result, security issues may be left unreported. security.txt defines a standard to help organizations define the process for security researchers to disclose security vulnerabilities securely."

Place a file security.txt on your website under the .well-known directory
Example https://www.bsi.bund.de/.well-known/security.txt

```
Contact: mailto:certbund@bsi.bund.de
Contact: https://www.bsi.bund.de/Security-Contact
Encryption: https://www.bsi.bund.de/Security-Contact
Preferred-Languages: de, en
Canonical: https://bsi.bund.de/.well-known/security.txt
Hiring: https://www.bsi.bund.de/Jobs
```

Not valid according to RFC 9116 !!!

Further info at

- https://datatracker.ietf.org/doc/html/rfc9116
- https://securitytxt.org

# Where to find CSAF documents?

| | |
|---|---|
| ✓ Valid CSAF documents<br>✓ File name restrictions<br>✓ TLS enforced<br>✓ TLP:WHITE freely accessible | CSAF publisher |
| ✓ Well-defined URL / security.txt / DNS => provider-metadata.json<br>✓ List of advisories and latest changes and Fixed folder structure<br>✓ or ROLIE feeds<br>✓ Restriction on >=TLP:AMBER<br>✓ All requirements from CSAF publisher | CSAF provider |
| ✓ Sign own advisories<br>✓ Hash advisories<br>✓ Published PGP keys for integrity checks<br>✓ All requirements from CSAF provider | CSAF trusted provider |

https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/prose/csaf-v2-editor-draft.md#7-distributing-csaf-documents

# Example: provider-metadata.json



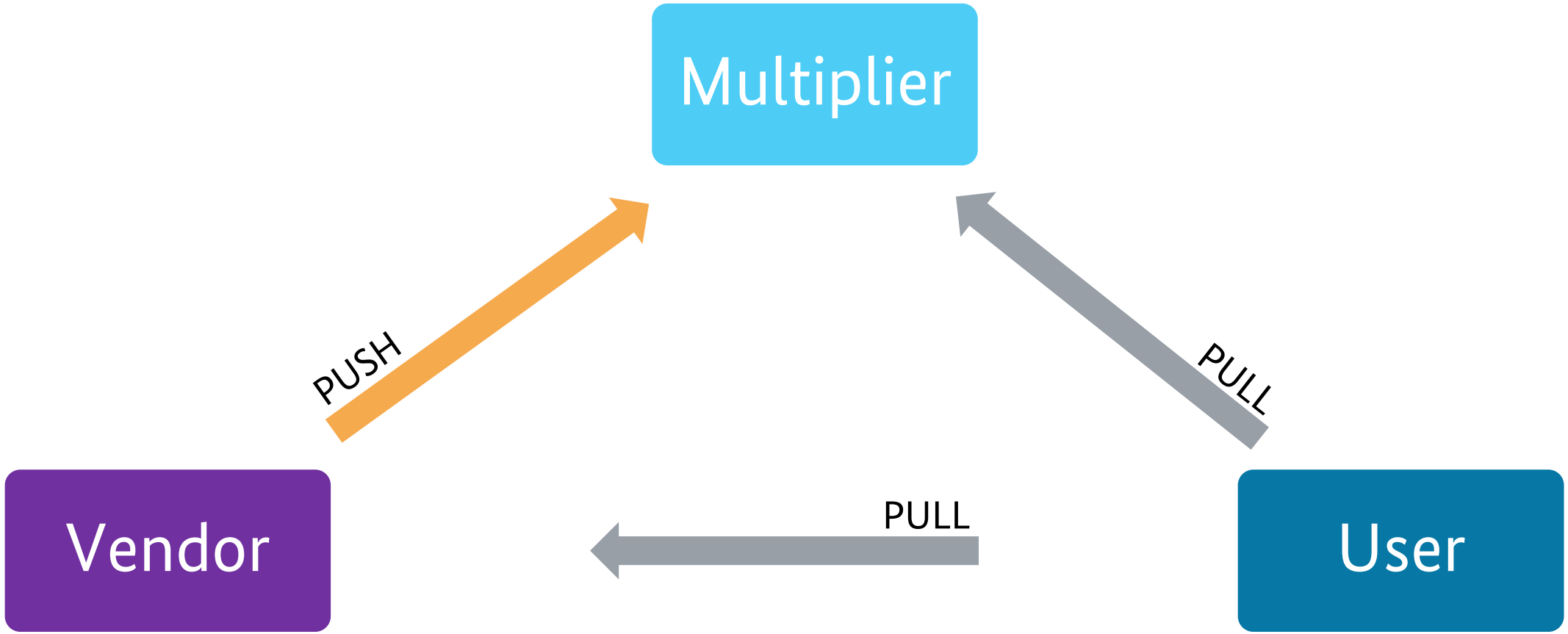
```json
{
  "canonical_url": "https://example01.test/.well-known/csaf/provider-metadata.json",
  "distributions": [
    {
      "rolie": {
        "feeds": [
          {
            "summary": "TLP:WHITE advisories",
            "tlp_label": "WHITE",
            "url": "https://example01.test/.well-known/csaf/white/csaf-feed-tlp-white.json"
          },
          {
            "summary": "TLP:GREEN advisories",
            "tlp_label": "GREEN",
            "url": "https://example01.test/.well-known/csaf/green/csaf-feed-tlp-green.json"
          },
          {
            "summary": "TLP:AMBER advisories",
            "tlp_label": "AMBER",
            "url": "https://example01.test/.well-known/csaf/amber/csaf-feed-tlp-amber.json"
          },
          {
            "summary": "TLP:RED advisories",
            "tlp_label": "RED",
            "url": "https://example01.test/.well-known/csaf/red/csaf-feed-tlp-red.json"
          }
        ]
      }
    }
  ],
  "last_updated": "2022-01-25T00:48:58Z",
  "list_on_CSAF_aggregators": true,
  "metadata_version": "2.0",
  "mirror_on_CSAF_aggregators": true,
  "public_openpgp_keys": [
    {
      "fingerprint": "ab6df118e05cd58a18ec96e315049730803d182c",
      "url": "https://example01.test/.well-known/csaf/openpgp/ab6df118e05cd58a18ec96e315049730803d182c.asc"
    }
  ],
  "publisher": {
    "category": "vendor",
    "name": "Example Company 01 ProductCERT",
    "namespace": "https://psirt.example.com"
  },
  "role": "csaf_trusted_provider"
}
```

# Example: ROLIE feed



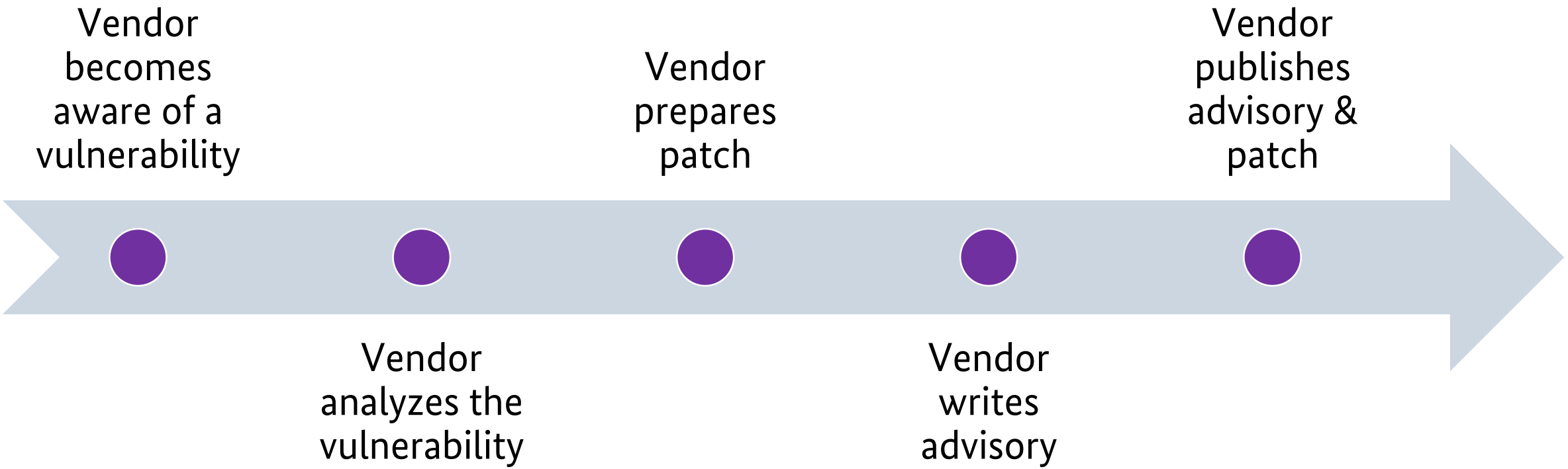
```
{
  "feed": {
    "id": "csaf-feed-tlp-white",
    "title": "CSAF feed (TLP:WHITE)",
    "link": [
      {
        "rel": "rel",
        "href": "https://example01.test/.well-known/csaf/white/csaf-feed-tlp-white.json"
      }
    ],
    "updated": "2022-04-08T23:46:56Z",
    "entry": [
      {
        "id": "2022-ESA-001",
        "title": "Example Security Advisory 2022/001",
        "link": [
          {
            "rel": "self",
            "href": "https://example01.test/.well-known/csaf/white/2022/2022-esa-001.json"
          },
          {
            "rel": "signature",
            "href": "https://example01.test/.well-known/csaf/white/2022/2022-esa-001.json.asc"
          },
          {
            "rel": "hash",
            "href": "https://example01.test/.well-known/csaf/white/2022/2022-esa-001.json.sha512"
          }
        ],
        "published": "2022-02-01T09:15:00Z",
        "updated": "2022-02-01T09:15:00Z",
        "content": {
          "type": "application/json",
          "src": "https://example01.test/.well-known/csaf/white/2022/2022-esa-001.json"
        },
        "format": {
          "schema": "https://docs.oasis-open.org/csaf/csaf/v2.0/csaf_json_schema.json",
          "version": "2.0"
        }
      },
      {
        "id": "2021-ESA-002",
        "title": "Example Security Advisory 002",
        "link": [
          {
            "rel": "self",
            "href": "https://example01.test/.well-known/csaf/white/2021/2021-esa-002.json"
```

# Eco System of Advisories

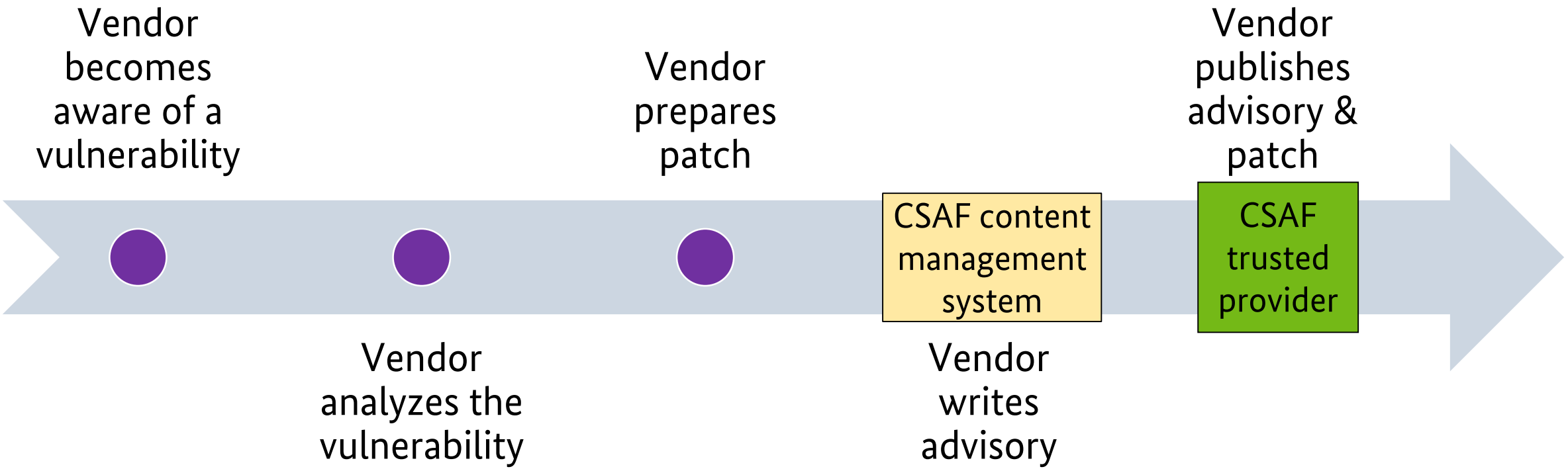


# Vendors’ Perspective

# Vendor


Vendor becomes aware of a vulnerability
Vendor analyzes the vulnerability
Vendor prepares patch
Vendor writes advisory
Vendor publishes advisory & patch

# Vendor


Vendor becomes aware of a vulnerability
Vendor analyzes the vulnerability
Vendor prepares patch
CSAF content management system
Vendor writes advisory
Vendor publishes advisory & patch
CSAF trusted provider

# Exercise 3

Retrieve a CSAF document

# Retrieving order

1. **Finding provider-metadata.json**
    1. Check Well-known URL (requirement 9 in section 7.1)
    2. Check security.txt (requirement 8 in section 7.1)
    3. Check DNS path (requirement 10 in section 7.1)
    4. Select one or more provider-metadata.json to use

2. **Retrieving CSAF documents**
    1. Parse provider-metadata.json: ROLIE-based (requirements 15 to 17 in section 7.1, preferred) or directory-based distribution (requirements 11 to 14 in section 7.1) to locate CSAF documents
    2. For CSAF trusted providers: retrieved hash and signature files (requirements 18 to 19 in section 7.1); check before further processing
    3. Test CSAF document against schema
    4. Execute mandatory tests

# How to know the main domain?

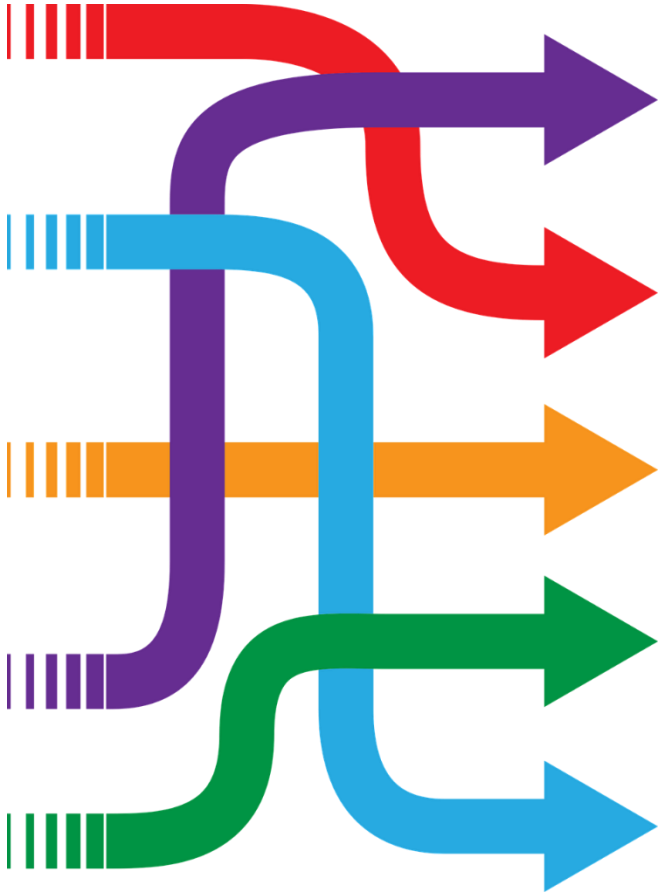
**CSAF Lister**

- Like telephone directory
- Lists known CSAF providers
- JSON structure

# Exercise 4

Update a CSAF document

# Everything perfect?

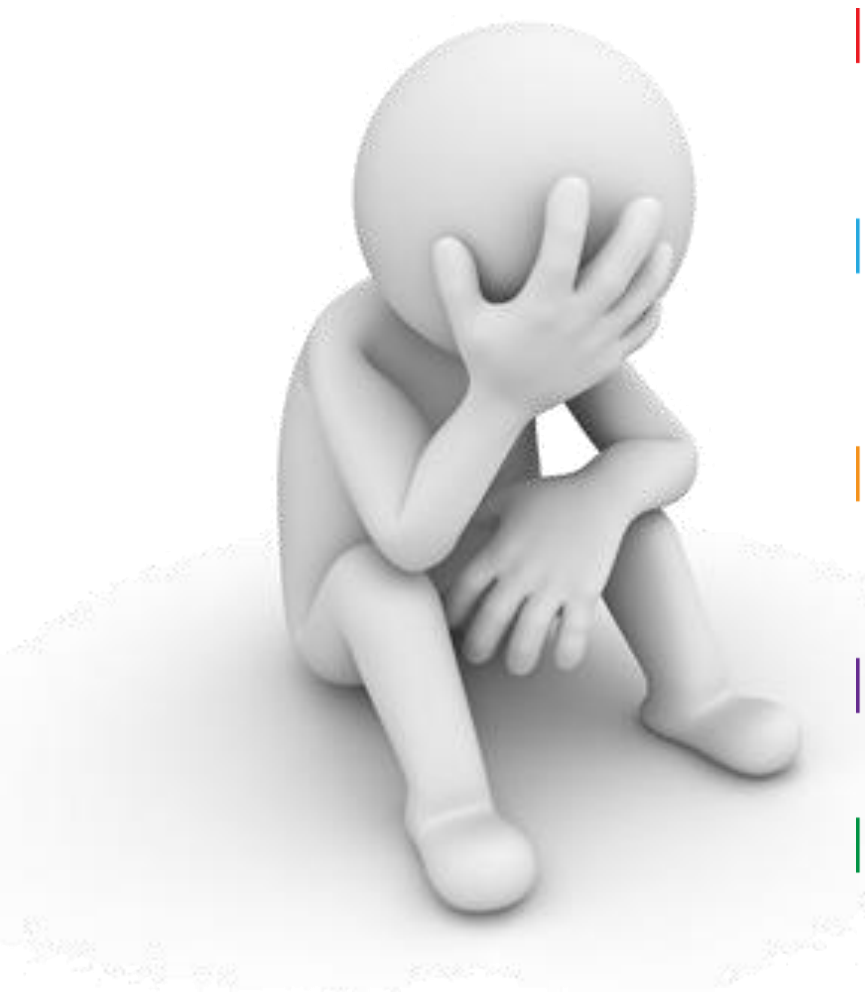


CSAF publisher

CSAF provider

CSAF trusted provider

# Obviously not! Still many sources of information



| | | | | | |
|---|---|---|---|---|---|
| CSAF publisher | CSAF publisher | CSAF publisher | CSAF provider | CSAF publisher | CSAF provider |
| CSAF publisher | CSAF publisher | CSAF trusted provider | CSAF publisher | CSAF provider | CSAF publisher |
| CSAF publisher | CSAF trusted provider | CSAF provider | CSAF provider | CSAF provider | CSAF trusted provider |
| CSAF trusted provider | CSAF trusted provider | CSAF trusted provider | CSAF provider | CSAF publisher | CSAF publisher |
| CSAF publisher | CSAF publisher | CSAF publisher | CSAF publisher | CSAF trusted provider | CSAF provider |
| CSAF trusted provider | CSAF provider | CSAF publisher | CSAF publisher | CSAF publisher | CSAF provider |
| CSAF trusted provider | CSAF trusted provider | CSAF trusted provider | CSAF trusted provider | CSAF provider | CSAF trusted provider |

Federal Office
for Information Security

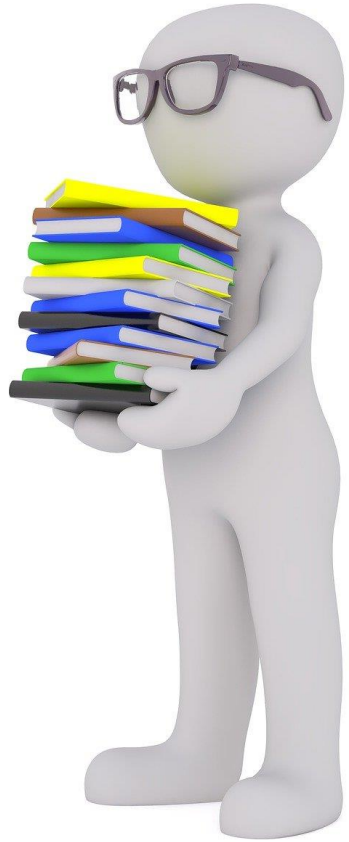
# One more step needed to make it easy …
# Saradi to the rescue!

CSAF aggregator

# Scalable and resilient advisory distribution infrastructure (Saradi)

## CSAF aggregator

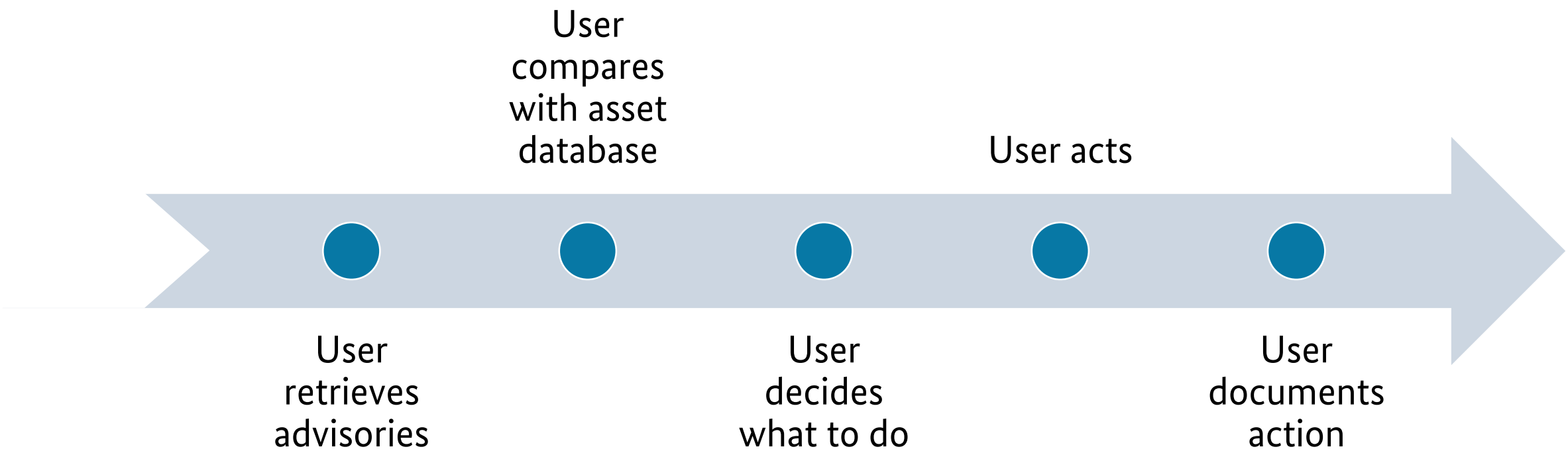
- Trusted party
- Collects advisories from issuers
- Provides them
- API optional
- One-stop-shop
- Multiple around the world (National CERTs)



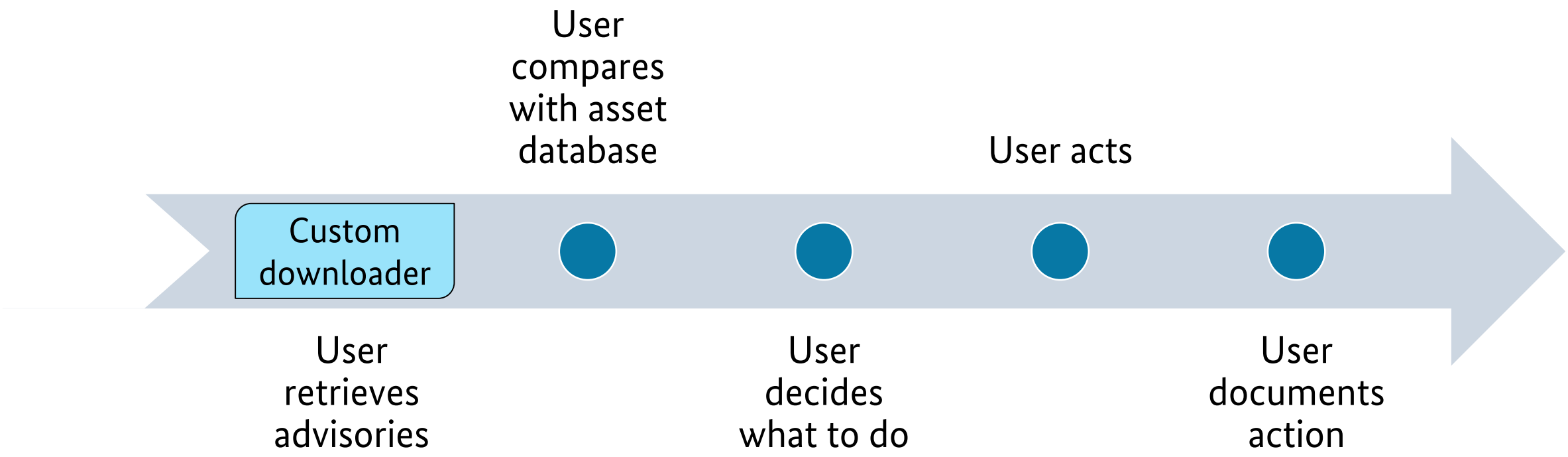
# Demo: CSAF Aggregator

# Users’ Perspective

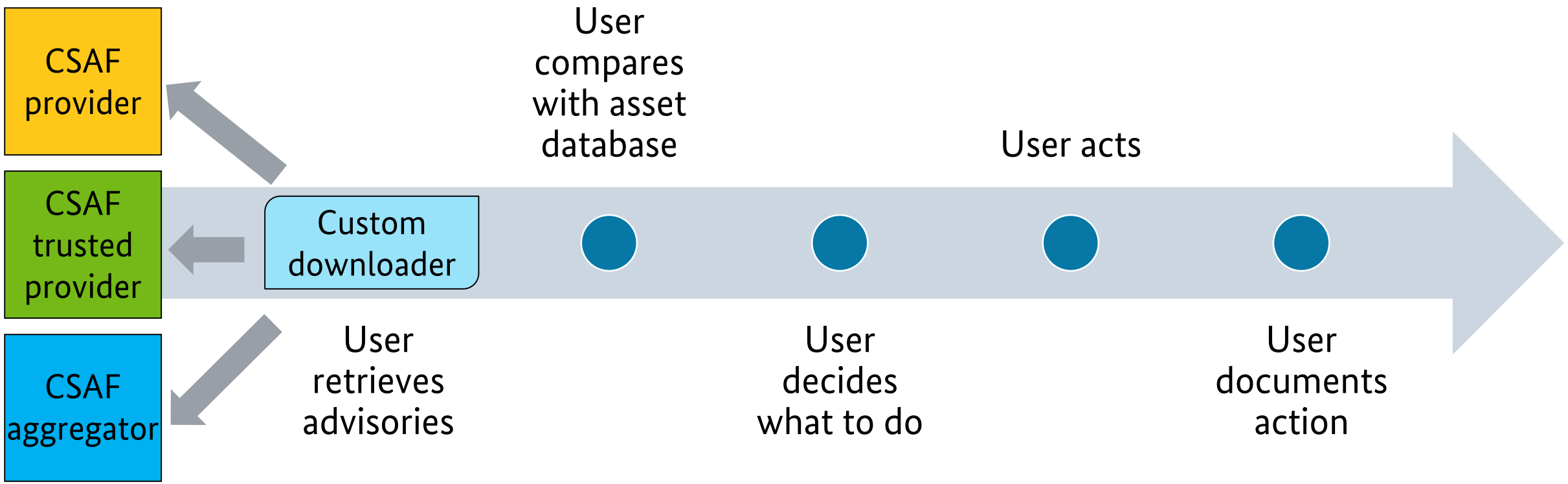
# User


User compares with asset database
User acts
User retrieves advisories
User decides what to do
User documents action

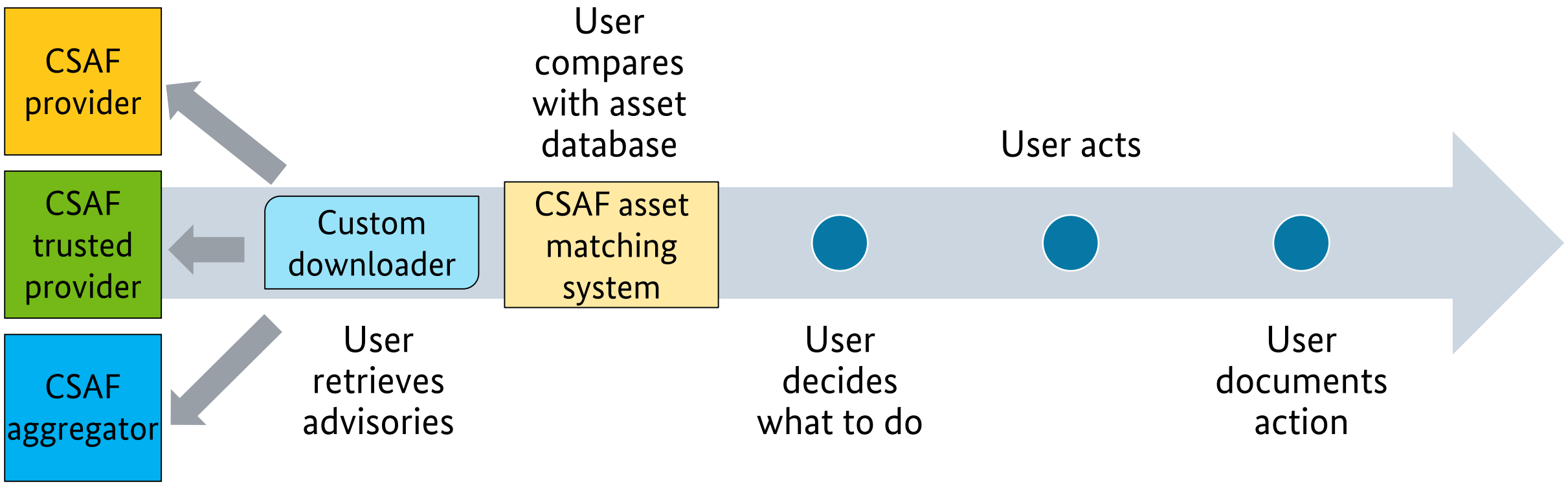
# User


User compares with asset database
User acts
Custom downloader
User retrieves advisories
User decides what to do
User documents action

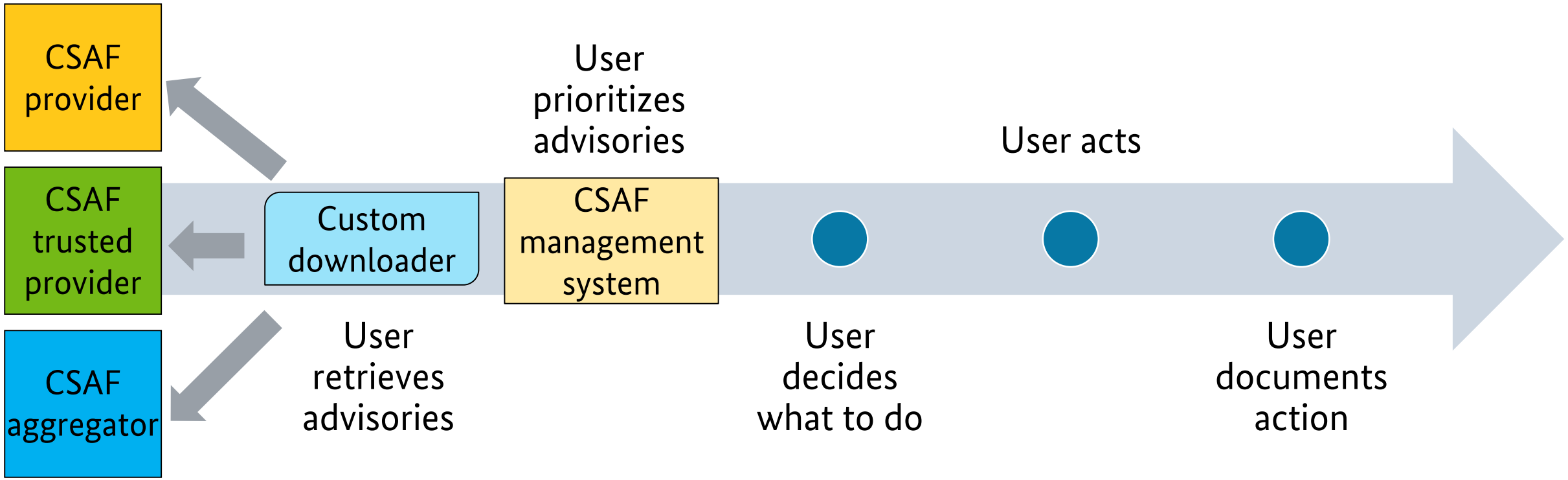
# User


CSAF provider
CSAF trusted provider
CSAF aggregator
Custom downloader
User retrieves advisories
User compares with asset database
User decides what to do
User acts
User documents action

# User


CSAF provider
CSAF trusted provider
CSAF aggregator
Custom downloader
User retrieves advisories
CSAF asset matching system
User compares with asset database
User decides what to do
User acts
User documents action

# User

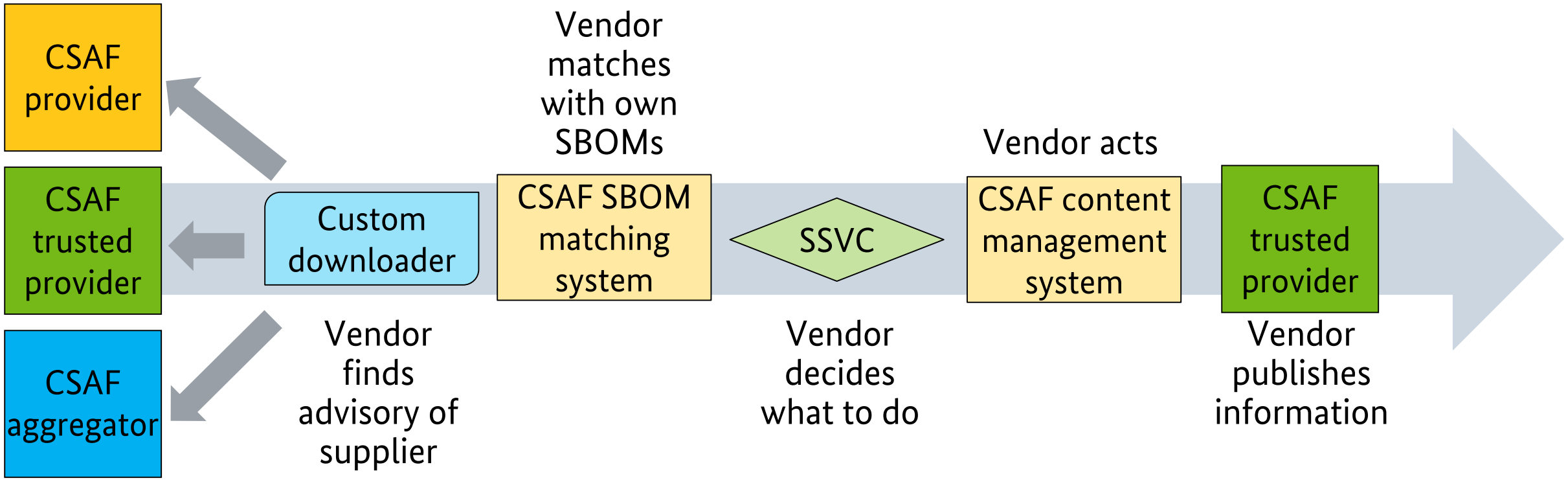

CSAF provider
CSAF trusted provider
CSAF aggregator
Custom downloader
User retrieves advisories
CSAF management system
User prioritizes advisories
User decides what to do
User acts
User documents action

# Bonus Exercise A

Push CSAF to ticket system or CSAF management system

# Supply chain: vendors’ view

# Supply chain



# Bonus Exercise B

Compare a CSAF document against an SBOM or asset database

# Exercise Compare a CSAF document against an SBOM or asset database

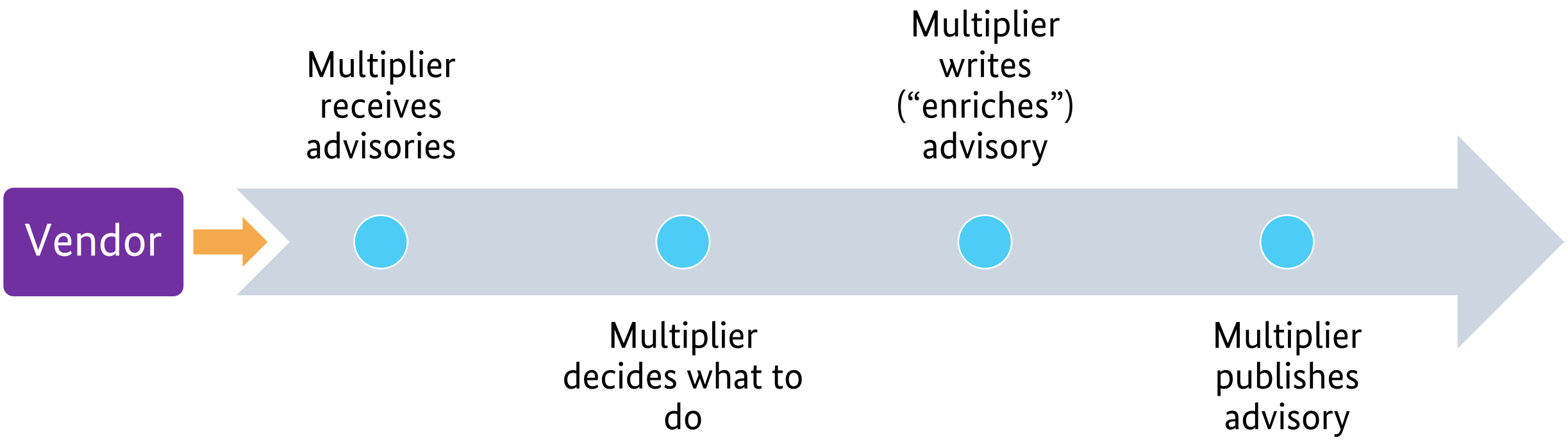
- Do it yourself later
- No software available at the moment
- Please tell us if you changed that

- Principles for matching
  - Input: match(product_tree, asset_database) or match(product_tree, sbom_database)
  - Output: for each product_id in product_tree: list of tuples (matched_asset_id, probability)

# Multiplier

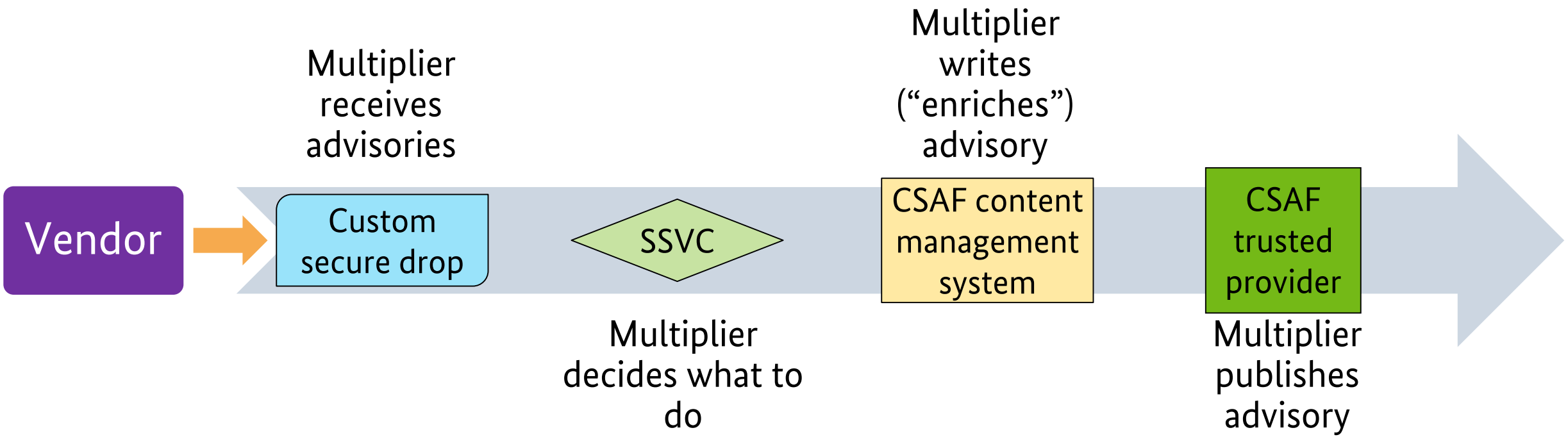
(Governmental) CERTs

# Multiplier

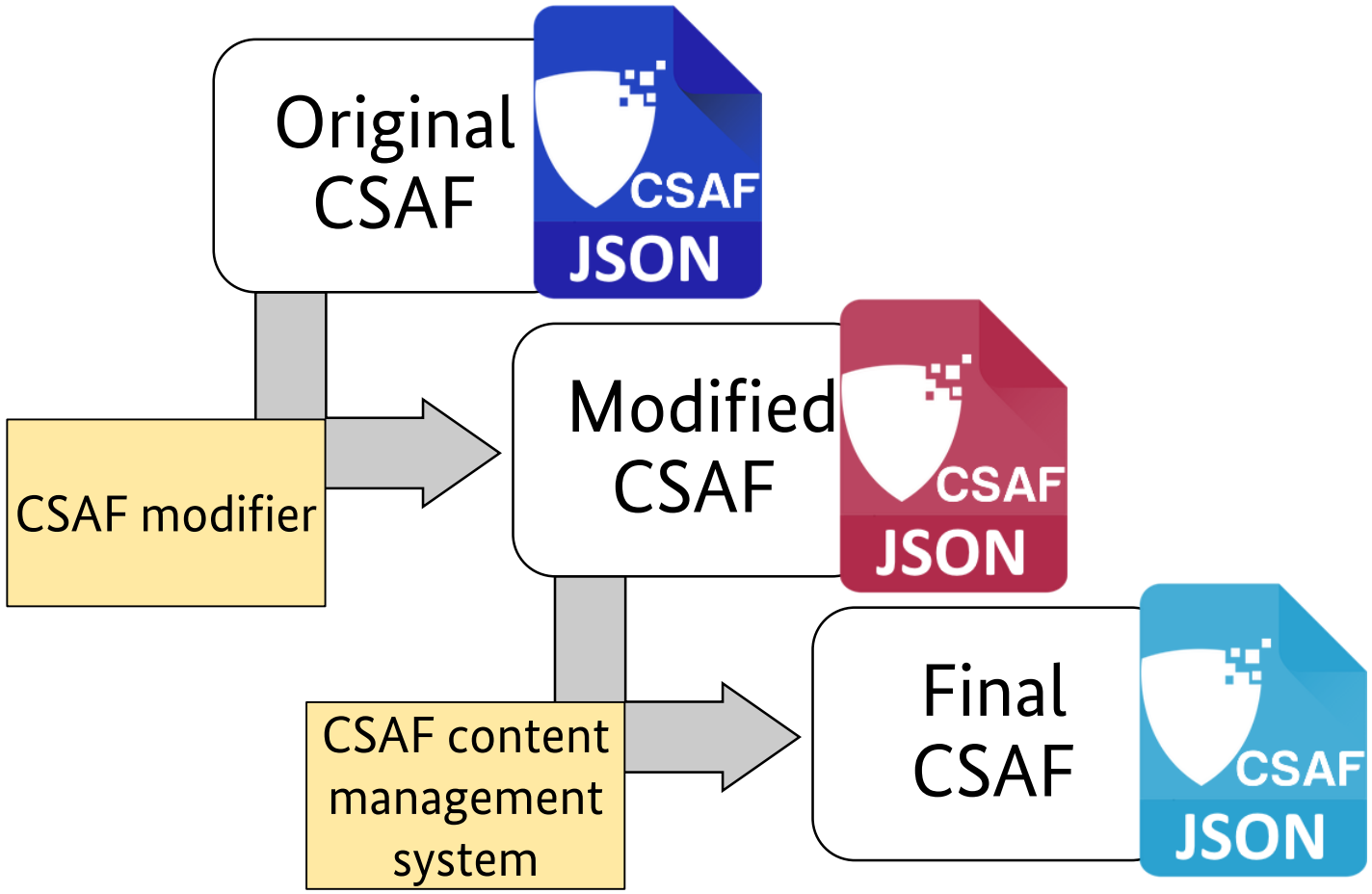



Federal Office for Information Security

# Multiplier


Multiplier receives advisories
Multiplier writes (“enriches”) advisory
Vendor
Custom secure drop
SSVC
CSAF content management system
CSAF trusted provider
Multiplier decides what to do
Multiplier publishes advisory

# Re-Use of existing information



# Bonus Exercise C

Modify a CSAF document programmatically

# CSAF modifier

The program:

- satisfies the "CSAF post-processor" conformance profile.
- adds, deletes or modifies at least one property, array, object or value of a property or item of an array.
- does not emit any objects, properties, or values which, according to section 9, are intended to be produced only by CSAF translators.
- satisfies the normative requirements given below.

The resulting modified document:

- does not have the same `/document/tracking/id` as the original document. The modified document can use a completely new `/document/tracking/id` or compute one by appending the original `/document/tracking/id` as a suffix after an ID from the naming scheme of the issuer of the modified version. It SHOULD not use the original `/document/tracking/id` as a prefix.
- includes a reference to the original advisory as first element of the array `/document/references[]`.

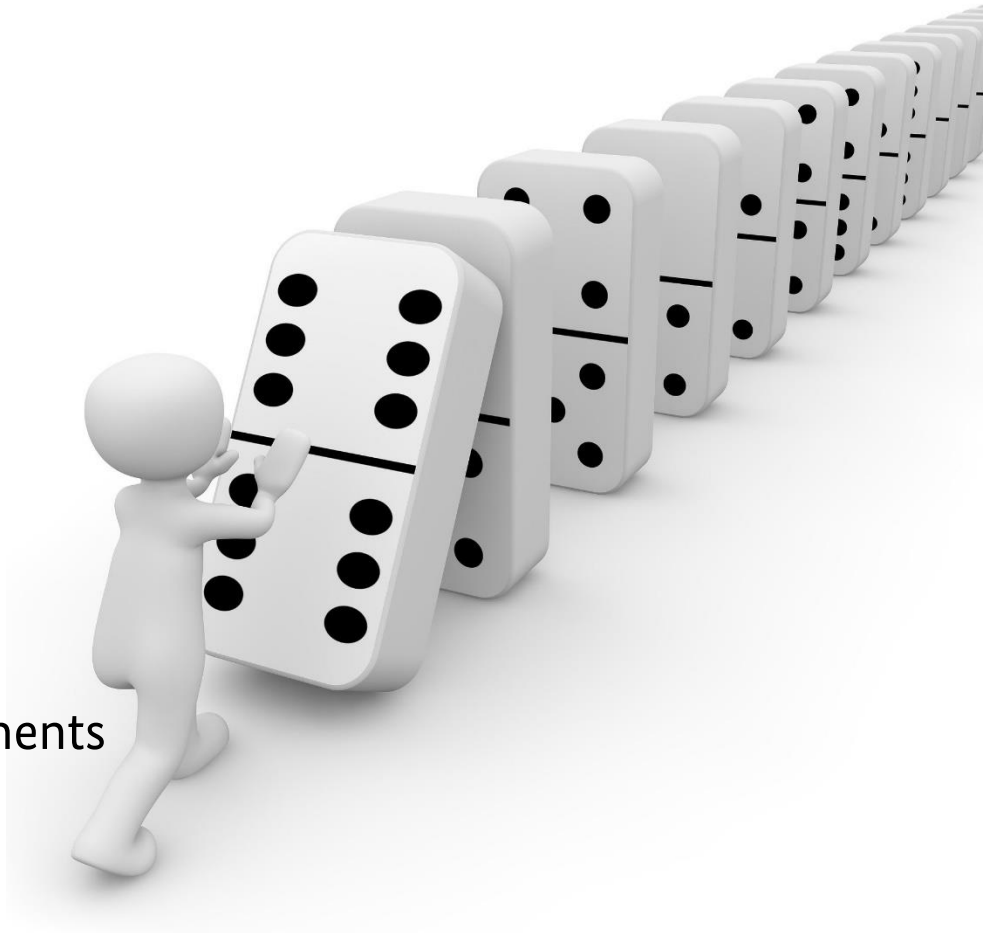
# Tools and more information

# Open Source tools in development

**Secvisogram**
- Generating CSAF documents based on a form
- Experts mode available

**Validator**
- Check whether given CSAF document is valid
- Provides additional remarks how to improve usability

**Domain checker**
- Tests whether given domain is (known to) distribute CSAF documents
- Checks which requirements are fulfilled



# Tools developed by the community

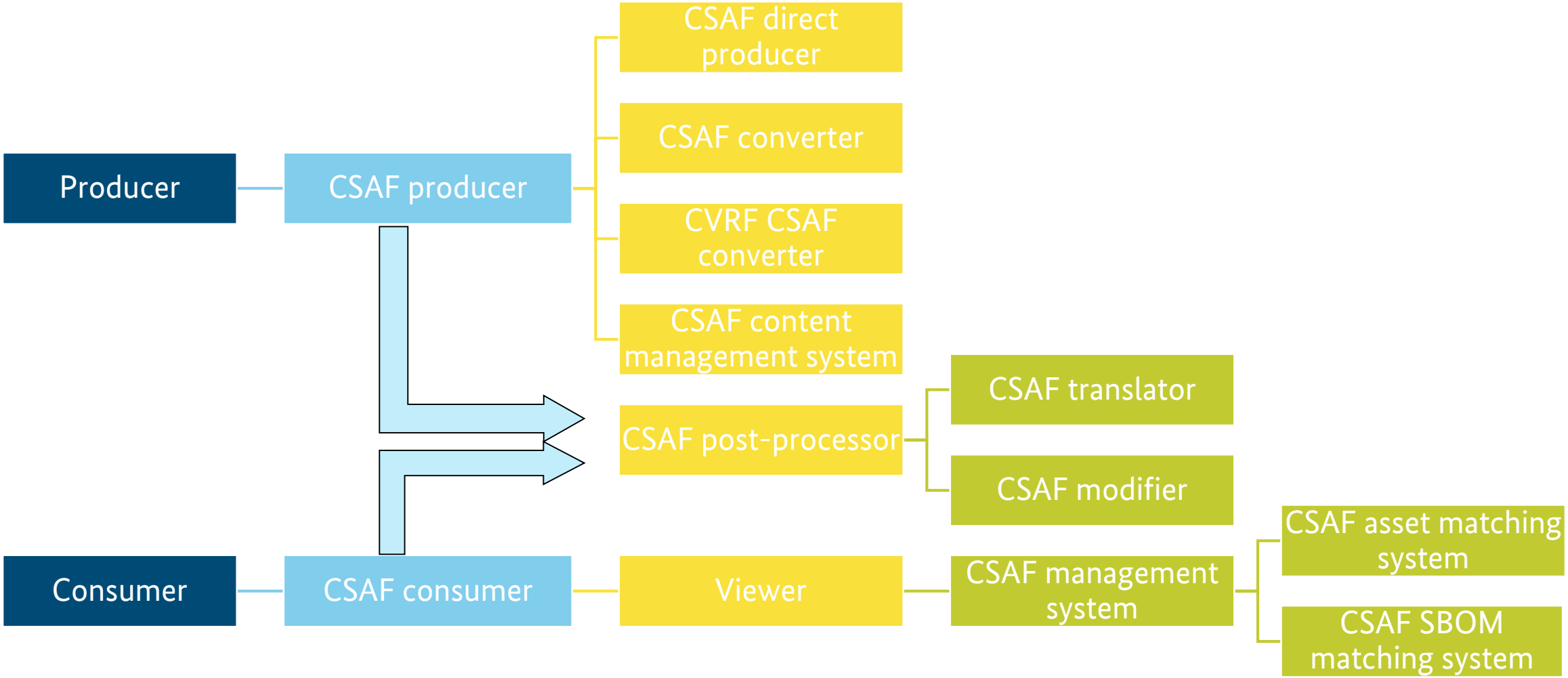
- CSAF producer: https://github.com/secvisogram/secvisogram
- CSAF content management system: https://github.com/secvisogram/secvisogram + https://github.com/secvisogram/csaf-cms-backend *(WIP)*
- CSAF trusted provider: https://github.com/csaf-poc/csaf_distribution *(WIP)*
- CSAF aggregator: https://github.com/csaf-poc/csaf_distribution *(WIP)*
- Provider checker: https://github.com/csaf-poc/csaf_distribution *(WIP)*
- CSAF management system: *open for commercial and Open Source tools*
- CSAF asset matching system: *open for commercial and Open Source tools*
- CSAF modifier: *custom implementation*
- CSAF downloader: https://github.com/csaf-poc/csaf_distribution *(WIP)*
- CSAF full validator: https://github.com/secvisogram/csaf-validator-lib (WIP)

- **Your tools?**

# Structure of CSAF 2.0 Specification

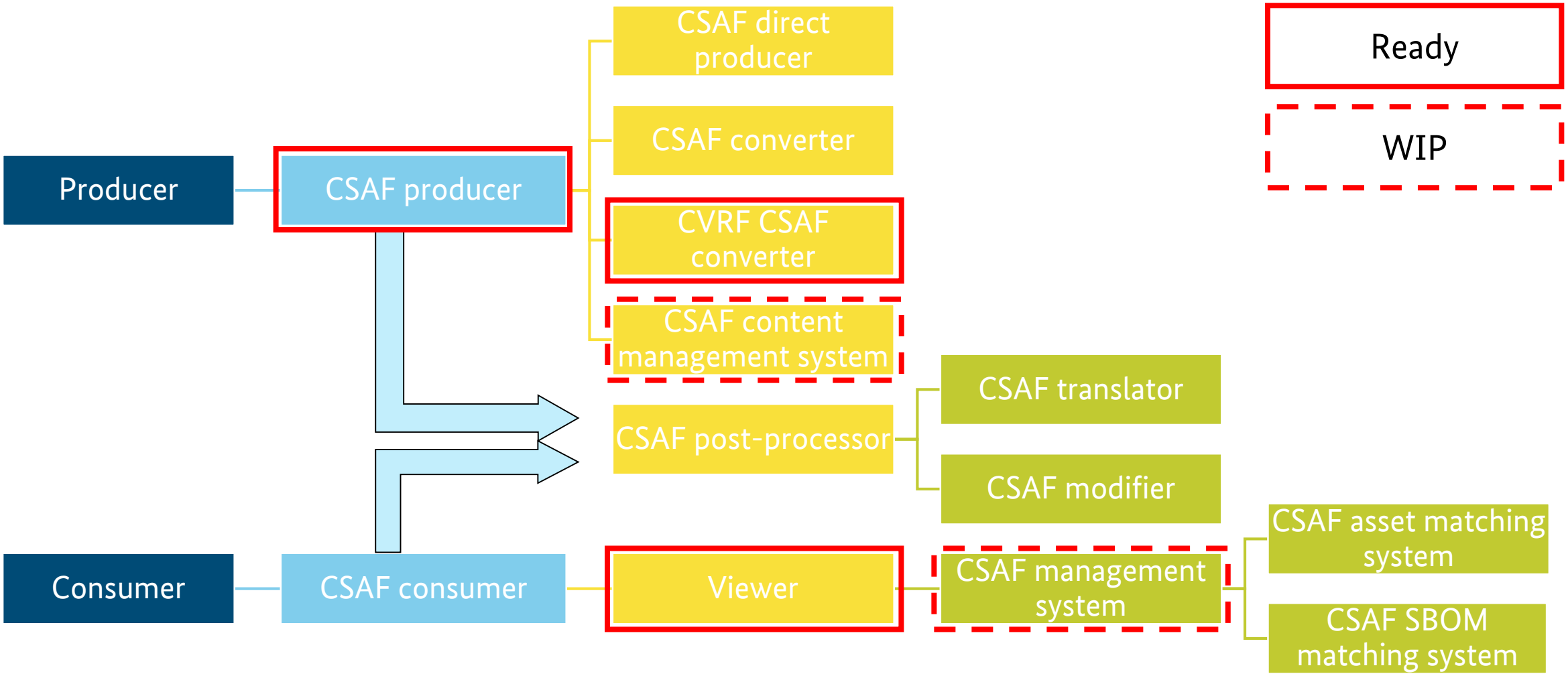
- Introduction & Design Considerations
- Schema elements
- Profiles
- Additional Conventions
- Tests
  - Mandatory
  - Optional
  - Informative
- Distributing CSAF documents
- Safety, Security, and Data Protection Considerations
- Conformance

# Specification of conformance targets – document level




https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/prose/csaf-v2-editor-draft.md#9-conformance

# Specification of conformance targets – document level




https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/prose/csaf-v2-editor-draft.md#9-conformance

# Where to find more information?

## https://csaf.io

| | |
|---|---|
| OASIS TC: CSAF website: | https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf |
| CSAF GitHub: | https://github.com/oasis-tcs/csaf |
| CSAF 2.0 JSON Schema: | https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/json_schema/csaf_json_schema.json |
| CSAF 2.0 Prose: | https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/prose/csaf-v2-editor-draft.md |
| CSAF 2.0 Examples: | https://github.com/oasis-tcs/csaf/tree/master/csaf_2.0/examples |
| Secvisogram sources: | https://github.com/secvisogram/secvisogram |
| Running Demo: | https://secvisogram.github.io |

# Open questions for CSAF 2.x & CSAF 3.0

- More automation
- API definition
- Distribution of advisories across aggregators
- Additional metrics like SSVC

- Solving the problem of unique product identifiers
- Improving integration of SBOM

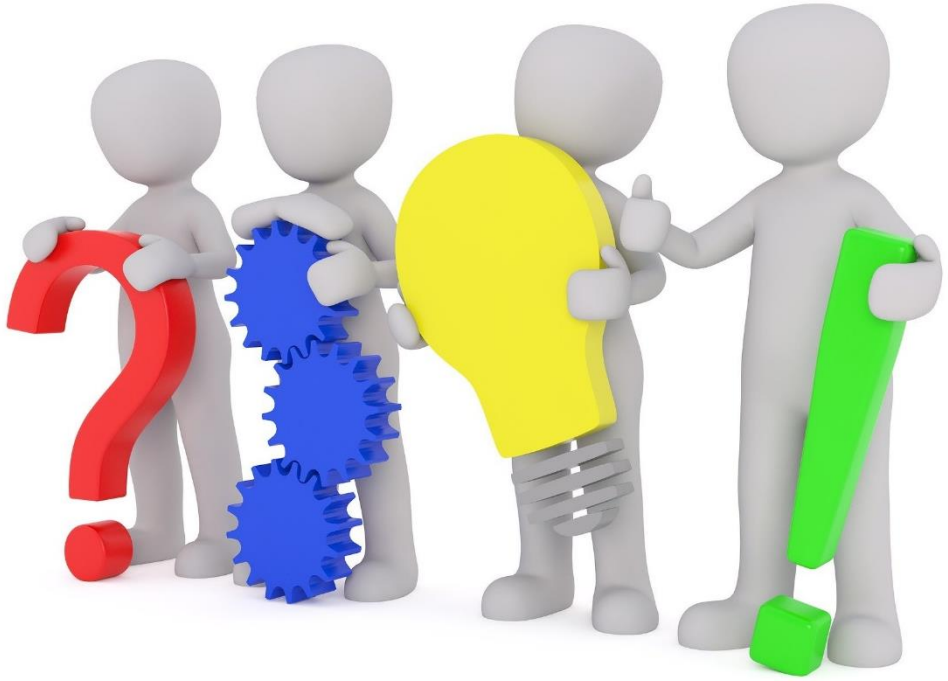
# Conclusions

# Summary

BSI continues its efforts

For success active support of many parties is required

- Adopt CSAF for own advisories
- Marketing
- Additional support tools
- Strong endorsement of CSAF towards
  - Vendors
  - Operators



What is your contribution?

# Key takeaways & actions

- Securing the supply chain is necessary
- You can't secure the supply chain on your own - it works only together
- Automation is possible and reduces human workload
- CSAF is a step towards a more secure supply chain through automation

- **Request your vendors to provide CSAF 2.0**
- **Provide CSAF documents to your customers to ease their pain**
- **Clean up your asset inventory / Setup SBOMs**
- **Spread the word! #oCSAF #advisory**

- *Don’t miss the presentation on VEX! (Thursday 11:20-11:55)*

Federal Office
for Information Security

Mr. Jens Wiesner Mr. Thomas Schmidt
Head of Section Subject Matter Expert
Industrial Automation and Control Systems

csaf@bsi.bund.de
Tel. +49 (0) 228 9582 6404
Fax +49 (0) 228 10 9582 6404
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de/dok/en_csaf